ŽILINSKÁ UNIVERZITA
V ŽILINE

MLADÁ VEDA 2025

XX. medzinárodná konferencia mladých vedeckých pracovníkov a doktorandov
14. – 15. apríl 2025
Žilina

Zborník článkov

PARTNERI

VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA BEZPEČNOSTNÍHO INŽENÝRSTVÍ

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

ŽILINSKÁ UNIVERZITA V ŽILINE
Fakulta bezpečnostného inžinierstva

ISBN: 978-80-554-2180-3
© Žilinská univerzita v Žiline, 2025
Vydavateľstvo: EDIS
Zborník je publikovaný v elektronickej podobe.

ŽILINSKÁ UNIVERZITA V ŽILINE
Fakulta bezpečnostného inžinierstva

Záštita nad konferenciou:

doc. Ing. Eva SVENTEKOVÁ, PhD. - dekanka Fakulty bezpečnostného inžinierstva, UNIZA, SR

Vedecký výbor konferencie:

Predseda výboru:

prof. Ing. Tomáš LOVEČEK, PhD. - Fakulta bezpečnostného inžinierstva, UNIZA, SR

Členovia:

Milan ADÁMEK – Univerzita Tomáše Bati ve Zlíně, Česká republika
Karla BARČOVÁ VŠB – Technická univerzita Ostrava, Česká republika
Aleš BERNATÍK VŠB – Technická univerzita Ostrava, Česká republika
Jacek DWORZECKI – Akadémia policajného zboru v Bratislave, Slovenská republika
Martin HROMADA – Univerzita Tomáše Bati ve Zlíně, Česká republika
Roman JAŠEK – Univerzita Tomáše Bati ve Zlíně, Česká republika
Petr KUČERA VŠB – Technická univerzita Ostrava, Česká republika
Marek KULCZYCKI – Uniwersytet Wrocławski, Polsko
Vladimír MÓZER – České vysoké učení technické v Praze, Česká republika
Balázs Vince NAGY Budapest University of Technology and Economics, Maďarsko
Jiří POKORNÝ VŠB – Technická univerzita Ostrava, Česká republika
Witalis PELLOWSKI – Akademia Wojsk Lądowych imienia generała T. Kościuszki, Polsko
Marzena PÓŁKA – Akademia Pożarnicza, Polsko
David ŘEHÁK VŠB – Technická univerzita Ostrava, Česká republika
Jozef RISTVEJ – Žilinská univerzita v Žiline, Slovenská republika
Marek RYBAKOWSKI – Uniwersytet Zielonogórski, Polsko
Eva SVENTEKOVÁ Žilinská univerzita v Žiline, Slovenská republika
Katarzyna TOBÓR-OSADNIK – Politechnika Śląska, Polsko
Jiří VOJTĚŠEK – Univerzita Tomáše Bati ve Zlíně, Česká republika

Organizačný výbor:

Ing. Lukáš VALLA - člen organizačného výboru, FBI, UNIZA, SR
Ing. Dušan BÓNA - člen organizačného výboru, FBI, UNIZA, SR
Ing. Samuel HUBOČAN - člen organizačného výboru, FBI, UNIZA, SR

Partnerské organizácie:

VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA BEZPEČNOSTNÍHO INŽENÝRSTVÍ

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Obsah

VÝVOJ NÍZKONÁKLADOVÉHO SENZORU PRO KONTINUÁLNÍ MONITOROVÁNÍ OXIDU DUSNÉHO 4
Melánie Barabášová[1], Václav Nevrlý[1], Michal Dostál[1], Vít Klečka[1], Petr Bitala[1], Jan Suchánek[2] 4

EXPERIMENTÁLNE OVERENIE SORPCIE VYBRANÝCH LÁTOK ZA POUŽITIA SORPČNYCH MATERIÁLOV 13
Dušan Bóna[1], Iveta Marková[1], Jozef Svetlík[1] 13

POŽIARNA BEZPEČNOSŤ EKOLOGICKÝCH IZOLAČNÝCH MATERIÁLOV: SKÚMANIE ICH VLASTNOSTÍ A DEGRADÁCIE 21
Dávid Boráros, Stanislava Gašpercová 21

TECHNOLOGICAL AND FIRE SAFETY ASPECTS OF ECOLOGICAL INSULATION MATERIALS PRODUCTION 28
Dávid Boráros[1], Stanislava Gašpercová[2] 28

RESILIENT COMPANIES 37
David Březina[1] 37

ČASOPROSTOROVÁ ANALÝZA KRIMINALITY POMOCÍ METODY NESTACIONÁRNÍHO KLOUZAVÉHO PRŮMĚRU 44
Karolina Dlouhá[1] 44

VLIV RASTROVÉHO PODHLEDU NA FUNKCI SPRINKLEROVÝCH HLAVIC 52
Michal Dvořák[1] 52

VLIV ŠÍŘKY DUTINY A POVRCHOVÉ ÚPRAVY DŘEVĚNÉ FASÁDY NA VÝŠKU PLAMENE 60
Stanisław Franek[1], Jakub Klezla[2], Michal Dvořák[3] 60

VLIV ZMĚNY VLASTNICTVÍ NA BEZPEČNOST ZAŘAZENÝCH OBJEKTŮ 67
Hana Halíčková[1], Michaela Skřížovská[2] 67

BEZPEČNOST V KOLABORATIVNÍ ROBOTICE 75
Kristýna Hamříková[1] 75

COMPARISON OF CONVOLUTIONAL NEURAL NETWORK ARCHITECTURES FOR EFFICIENT FACE RECOGNITION IN SECURITY PRACTICE 83
Martin Haváček[1] 83

IMPLEMENTÁCIA POŽIARNEHO MODELOVANIA DO PRAXE 92
Dorota Hodúlová[1], Stanislava Gašpercová[2] 92

SITUATIONAL PREVENTION AS A TOOL FOR THE PROTECTION OF SOFT TARGETS WITH A FOCUS ON SCHOOLS AND SCHOOL FACILITIES 101
Samuel Hubočan[1], Viktor Šoltés[2], Veronika Adamová[3] 101

POŽIARNA OCHRANA VYBRANÝCH KULTÚRNYCH DREVENÝCH SAKRÁLNYCH PAMIATOK V OKRESE SOBRANCE 111
Michal Huliak[1], Iveta Marková[2] 111

DÁTOVÝ RÁMEC POSUDZOVANIA RIZÍK PREPRAVY NEBEZPEČNÝCH LÁTOK CESTNOU DOPRAVOU A NÁVRH KONCEPTU ECALL PRE PODPORU ZÍSKAVANIA INFORMÁCIÍ V REÁLNOM ČASE 120
Boris Kollár[1], Daniel Chovanec[2] a Karin Nováková[3] 120

MIKROPLASTY V HASEBNÍCH VODÁCH 128
Lucie Králová[1], Karla Barčová[2], Petr, Adamus[3] 128

APLIKÁCIA KORELAČNEJ ANALÝZY NA STAVEBNOTECHNICKÝ STAV MOSTOV NA SLOVENSKU 136
Michal Miške[1] 136

OCHRANA A TECHNICKÉ ZABEZPEČENÍ MALÝCH MODULÁRNÍCH JADERNÝCH ELEKTRÁREN V RÁMCI KRITICKÉ INFRASTRUKTURY ČR 144
Aleš Navrátil[1] 144

THE IMPACT OF NIS2 DIRECTIVE ON THE RESILIENCE OF CRITICAL INFRASTRUCTURE ENTITIES 152
Mimi Enakome Oka[1], Martin Hromada[2], Roman Jasek[3] 152

MOŽNOSTI ZVYŠOVANIA BEZPEČNOSTI NA ELEKTRIČKOVÝCH TRATIACH 161
Peter Onderčo[1], Jan Rybář[2], Jozef Leja[3] 161

LABORATORNÍ ŘÁD A BEZPEČNOST PRÁCE V LABORATOŘI MEDICÍNSKÉ METROLOGIE 170
Jan Rybář[1], Jozef Leja[2] 170

DETERMINANTY SPOLEHLIVOSTI STAVEBNÍCH KONSTRUKCÍ SILNIČNÍ KRITICKÉ INFRASTRUKTURY 178
Ondřej Ryška[1] 178

VEDE POUŽÍVÁNÍ POHYBOVÝCH SNÍMAČŮ KE SNÍŽENÍ VÝSKYTU MSD NA PRACOVIŠTI? 184
Karolína Šablaturová[1] 184

ANALÝZA SKORONEHOD A SCÉNÁŘŮ VEDOUCÍCH K VÁŽNÝM PRACOVNÍM ÚRAZŮM 189
Kristýna Schneiderová[1] 189

FIREFIGHTER PERCEPTION OF RISK: APPLICATION OF A QUESTIONNAIRE SURVEY IN THE CZECH REPUBLIC 197
Patrik Sirotiak[1] 197

VYUŽITIE VNÚTORNÝCH POLOHOVACÍCH SYSTÉMOV V RÁMCI INFORMAČNEJ BEZPEČNOSTI 205
Erika Skýpalová[1], Martin Boroš[2] 205

„POST-MARKET CLINICAL FOLLOW-UP“ AKO NÁSTROJ BEZPEČNOSTI V ZDRAVOTNÍCTVE 213
Andrej Smetánka[1], Jan Rybář[2], Jana Gerneschová[3] 213

EXPLOITING TRUST: HOW SOCIAL ENGINEERING THRIVES AND WHY ZERO TRUST MODEL MIGHT BE THE SOLUTION 222
Marek Švaňhal[1] 222

EXPERIMENTÁLNÍ URČENÍ OPTIMÁLNÍHO PODTLAKU PRO MĚŘENÍ VE VÝBUCHOVÉM AUTOKLÁVU VA–250L 230
Kateřina Symonová[1] 230

OVERVIEW OF AUTONOMOUS TRAIN SYSTEMS AND THEIR SAFETY UP TO GRADE OF AUTOMATION (GOA) 4 238
Martin Václavík[1], Martin Haváček[2] 238

ANALÝZA VÝJAZDOV ZDRAVOTNEJ ZÁCHRANNEJ SLUŽBY NA SLOVENSKU A VÝVOJOVÉ TRENDY 246
Lukáš Valla[1] 246

MOŽNOSTI ZVÝŠENÍ ÚROVNĚ ZABEZPEČENÍ BUDOV MĚSTSKÝCH ÚŘADŮ PŘED HROZBOU ÚTOKU AKTIVNÍHO STŘELCE 254
Ondřej Velísek[1] 254

VÝVOJ NÍZKONÁKLADOVÉHO SENZORU PRO KONTINUÁLNÍ MONITOROVÁNÍ OXIDU DUSNÉHO

Melánie Barabášová[1], Václav Nevrlý[1], Michal Dostál[1], Vít Klečka[1], Petr Bitala[1], Jan Suchánek[2]

ABSTRAKT

Tento příspěvek se zaměřuje na vývoj nízkonákladového senzoru oxidu dusného (N_2O) na bázi NDIR technologie, určeného pro kontinuální monitorování a včasnou detekci N_2O. Senzor, využívající platformu ESP32 pro sběr a přenos dat, umožňuje detekci koncentrací N_2O nad 1 ppm, což je klíčové pro prevenci havárií spojených s tepelným rozkladem dusičnanu amonného. Testy v laboratorních a terénních podmínkách ukázaly nízkou interferenci CO_2 (<8 % signálu) a chybu měření pod 3 %. Přesnost systému lze zlepšit kombinací s CO_2 a CO senzory a použitím korekčních algoritmů. Tento cenově dostupný systém představuje efektivní alternativu k QCL metodám a nástroj pro monitorování environmentálních rizik.

Klíčové slova:
Oxid dusný; NDIR technologie; nízkonákladový senzor; kontinuální monitoring

ABSTRACT

This paper focuses on the development of a low-cost nitrous oxide (N_2O) sensor based on NDIR technology for continuous monitoring and early detection of N_2O. The sensor, using the ESP32 platform for data acquisition and transmission, enables the detection of N_2O concentrations above 1 ppm, which is key to preventing accidents associated with the thermal decomposition of ammonium nitrate. Tests in laboratory and field conditions have shown low CO_2 interference (<8 % of the signal) and a measurement error below 3 %. The accuracy of the system can be improved by combining it with CO_2 and CO sensors and using correction algorithms. This affordable system is an effective alternative to QCL methods and a tool for monitoring environmental risks.

Key words:
Nitrogen oxide; NDIR technology; low cost sensor; continuous monitoring

1 Ing. Melánie Barabášová, Fakulta bezpečnostního inženýrství, Vysoká škola báňská – Technická univerzita Ostrava, Lumírova 630/13, 700 30 Ostrava-Výškovice, Česká republika, melanie.barabasova@vsb.cz
2 Ing. Jan Suchánek, Ph.D., Ústav fyzikální chemie J. Heyrovského AV ČR, v. v. i., Dolejškova 2155/3, 8, 182 23 Praha, Česká republika

1 ÚVOD

Oxid dusný (N_2O) je významný skleníkový plyn, který navíc hraje klíčovou roli v poškozování ozonové vrstvy vlivem jeho zvýšené reaktivity ve stratosféře. Průměrná doba života oxidu dusného v atmosféře se pohybuje okolo 150 let, přičemž vlivem fotochemických reakcí v prostředí stratosféry narušuje ozonovou vrstvu [1]. Chemická reakce s atomárním kyslíkem spouští cyklus deplece ozónu (O_3) uvedený v následujících chemických rovnicích (1–3):

$$N_2O + O \rightarrow 2NO \tag{1}$$
$$NO + O_3 \rightarrow NO_2 + O_2 \tag{2}$$
$$NO_2 + O \rightarrow NO + O_2 \tag{3}$$

Z globální perspektivy pocházejí emise oxidu dusného (N_2O) z různorodých zdrojů, mezi něž patří:

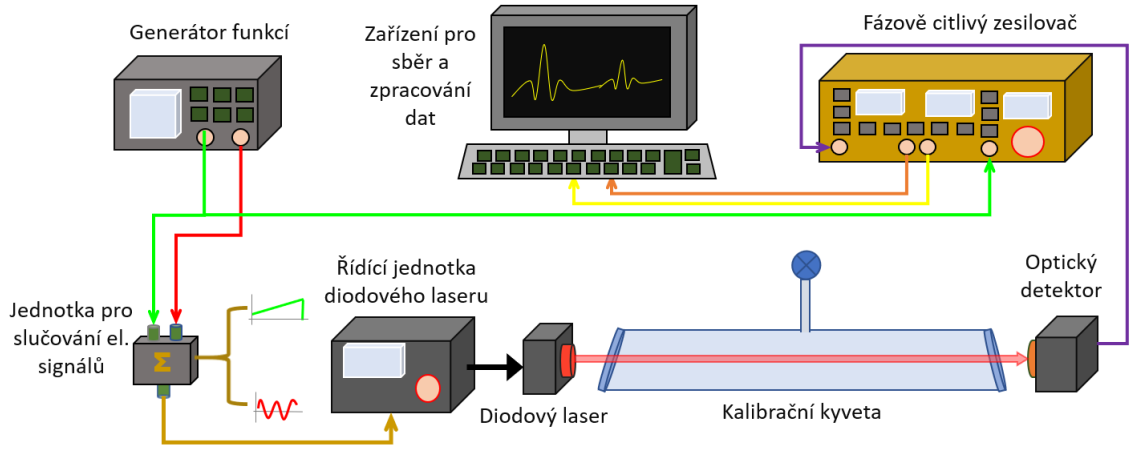
- **Zemědělství:** Aplikace dusíkatých hnojiv, zejména dusičnanu amonného (NH_4NO_3), jehož samovolná degradace v minulosti vedla k několika závažným průmyslovým haváriím. Chov hospodářských zvířat, při kterém dochází k produkci N_2O v důsledku mikrobiálních procesů probíhajících v půdě a trávicím traktu zvířat.
- **Průmyslové procesy:** Výroba chemických látek, zejména kyseliny dusičné a kaprolaktamu, při níž je N_2O emitován jako vedlejší produkt.
- **Povrchová těžba:** Použití dusičnanu amonného v průmyslových výbušninách, které během reakce vedou k uvolňování oxidu dusného [2].
- **Spalovací procesy**: Oxid dusný vzniká při spalování fosilních paliv v sektoru dopravy, energetiky a průmyslu. Významným zdrojem emisí mohou být také lesní požáry, které ovlivňují koloběh dusíku a přispívají ke znečištění ovzduší. Dále vzniká jako nežádoucí vedlejší produkt při spalování amoniaku a představuje závažné environmentální riziko vzhledem ke svému vysokému potenciálu globálního oteplování a schopnosti narušovat ozonovou vrstvu [3].

Tradiční metody detekce N_2O, jako plynová chromatografie a FTIR spektroskopie, mají omezenou přenositelnost a vysoké provozní náklady, což ztěžuje jejich využití v terénním monitorování. Alternativou jsou kvantově-kaskádové lasery (IR-QCL), které poskytují vysokou citlivost a selektivitu, ale jejich vysoká cena a nároky na obsluhu limitují širší použití. Vyvíjejí se opticky založené senzory pro kontinuální a dostupnější monitorování, zejména v zemědělství, kde N_2O vzniká při aplikaci dusíkatých hnojiv. [4] Pro sledování emisí N_2O se rovněž využívají satelitní měření, ale ta postrádají dostatečnou citlivost pro detekci v nejnižší troposféře. Vytvoření husté sítě pozemních stanic by mohlo doplnit satelitní data, zpřesnit odhady emisí a zlepšit dlouhodobé monitorování N_2O, což by přispělo k efektivnějším strategiím mitigace a zlepšení environmentální politiky [5].

2 SPEKTROSKOPICKÁ DETEKCE N_2O S VYUŽITÍM IR-QCL (ANALÝZA STOPOVÝCH KONCENTRACÍ V LABORATORNÍCH PODMÍNKÁCH)

Při použití polovodičových laserů pro metody detekce plynů je nutná jejich kalibrace. Proces kalibrace spočívá v měření absorpčního spektra druhé harmonické (2*f*) referenčního plynu v infračervené oblasti a následném přiřazení spektrálních absorpčních linií k odpovídajícím liniím daného plynu, získaným z databáze infračervených absorpčních spekter HITRAN. Výběr referenčního plynu pro kalibraci diodového laseru je realizován s ohledem na dostatečný počet absorpčních linií v dané spektrální oblasti, jejich různou intenzitu a dostupnost odpovídajících spektrálních dat v databázi infračervených spekter [6].

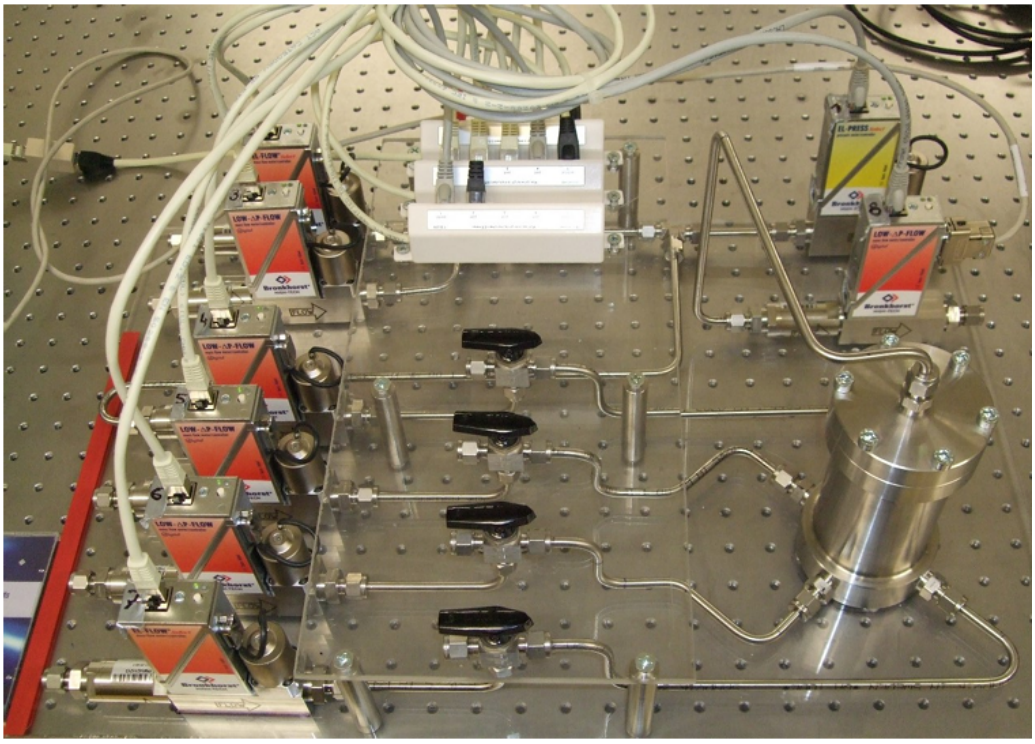
Experimentální uspořádání sestavy zahrnuje diodový laser, kyvetu s referenčním plynem nebo laminární proud plynu, fotodetektor a elektronická zařízení pro řízení laseru a zpracování signálu z fotodetektoru (Obrázek 1). Kalibrace kvantově kaskádového laseru (QCL) Thorlabs QC 4580 probíhala s oxidem dusným v kyvetě o délce 500 mm. Intenzita laserového svazku byla měřena fotodetektorem InSb s předzesilovačem DP 8100. Teplota laseru byla stabilizována na 25 °C a modulace řízena generátorem EZ FG-7005C. Plynulé ladění vlnové délky bylo prováděno počítačem řízeným asymetrickým trojúhelníkovým signálem. Detekovaný signál byl demodulován fázově citlivým zesilovačem (Lock-in) Stanford Research SR830DSP a zesílen 10×. Výsledná data byla převedena do digitální podoby a uložena do počítače [6].



Obrázek 1 Experimentální sestava pro kalibraci diodových laserů

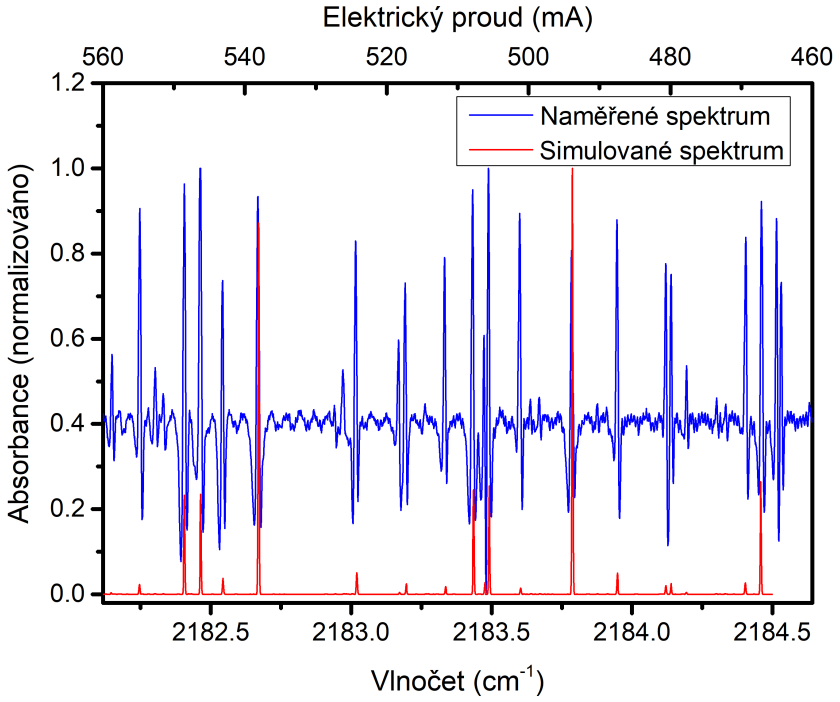
Pro provedení tzv. laboratorní kalibrace je důležitá sestava průtokoměrů (Obrázek 2). Hlavním účelem této sestavy je příprava směsí s definovanými koncentracemi, což umožňuje stanovení měřicího rozsahu jednotlivých detekčních zařízení. Sestava je složena ze sedmi průtokoměrů (různé průtoky: 25 ml/min, 500 ml/min, 1000 ml/min vzduchu), které zajišťují měření průtoku s malými rozdíly tlaku. Dále je v sestavě mixážní komůrka jejíž účelem je

zajištění homogenní plynné směsi o jakékoliv koncentraci, regulátor tlaku, směšovací komora a zdroj [7].



Obrázek 2 Sestava pro vytváření definovaných směsí [7]

Srovnání naměřeného a simulovaného absorpčního spektra v laboratorních podmínkách je znázorněno na Obrázku 3. Osa x udává vlnočet v cm^{-1}, přičemž byla přidána horní osa x, která vyjadřuje závislost vlnočtu (vlnové délky) na elektrickém proudu protékajícím polovodičovým laserem. Osa y reprezentuje normalizovanou absorbanci, tedy míru absorpce záření v daném spektrálním rozsahu. Modrá křivka odpovídá naměřenému spektru, zatímco červená křivka zobrazuje simulované spektrum získané na základě teoretických modelů z databáze HITRAN [8]. Z grafu je patrné, že pozice absorpčních čar v naměřeném spektru dobře koresponduje se simulovanými hodnotami, což potvrzuje správnost kalibrace a spektrálního přiřazení. Důležitou součástí analýzy je také horní osa x, která zobrazuje závislost vlnočtu na elektrickém proudu protékajícím laserovou diodou. Tento vztah umožňuje přesné ladění vlnové délky emitovaného záření změnou elektrického proudu. Přesnost simulace a shoda absorpčních čar s naměřenými hodnotami demonstrují správnou funkci metody použité pro kalibraci laseru.

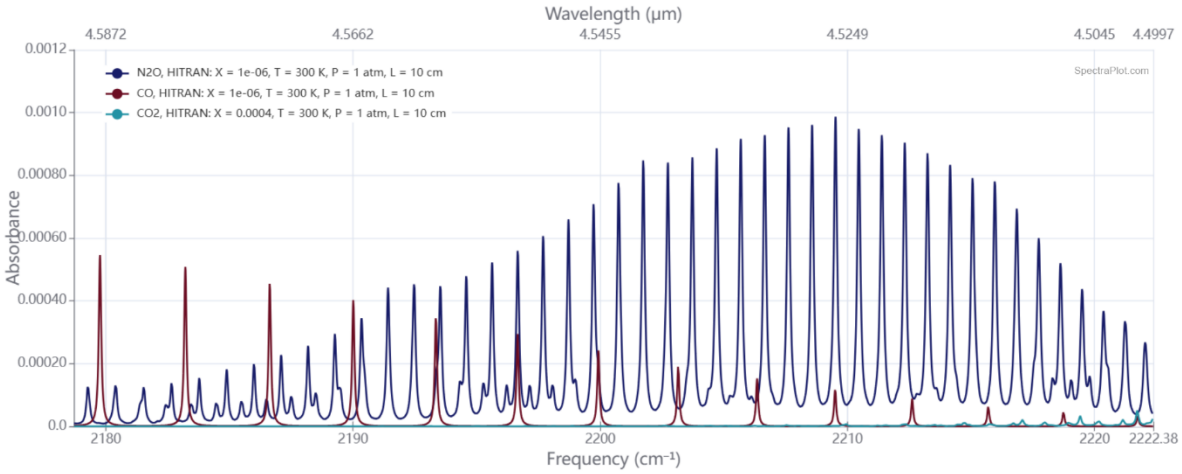


Obrázek 3 Porovnání naměřeného absorpčního spektra N_2O za sníženého tlaku (cca 10 Torr) se spektrem simulovaným

3 NDIR SENZOR (SMARTGAS) A INTEGRACE S IOT MODULEM (ŘEŠENÍ SBĚRU A VIZUALIZACE DAT

Zaměřením této studie je na praktickou implementaci kontinuálního monitoringu pomocí nedisperzivní infračervené (NDIR) technologie a její integraci s IoT infrastrukturou. Toto propojení představuje významný krok mezi laboratorní analýzou a terénním měřením, které je nezbytné pro efektivní monitoring emisí N_2O v environmentálně významných lokalitách. Nedisperzivní infračervená spektroskopie (NDIR) představuje alternativní přístup k detekci plynů, který se vyznačuje nižšími náklady a vyšší robustností ve srovnání s metodami využívajícími kvantově kaskádové lasery. Na rozdíl od IR-QCL technologie diskutované v kapitole 2, NDIR senzory nevyžadují precizní teplotní stabilizaci ani složité optické sestavy, což je činí vhodnými pro terénní aplikace a dlouhodobý kontinuální monitoring.

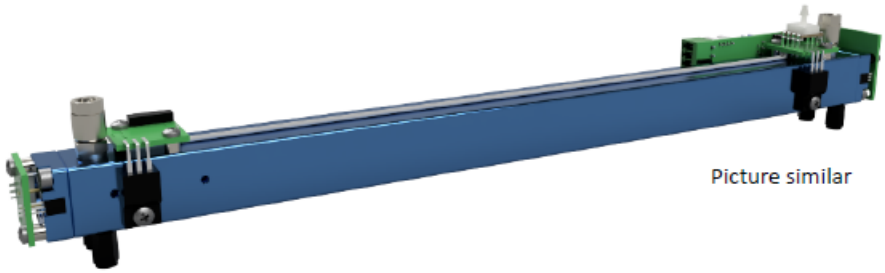
Princip NDIR senzorů spočívá v měření absorpce širokopásmového infračerveného záření při průchodu analyzovaným plynem. Tato metoda, ačkoliv poskytuje nižší spektrální rozlišení než QCL technologie, nabízí dostatečnou selektivitu pro detekci N_2O v atmosférických koncentracích při správné volbě optických filtrů a detekčních parametrů. Klíčovou výhodou NDIR technologie je její schopnost operovat v širokém rozsahu environmentálních podmínek s minimálními nároky na údržbu. NDIR technologie pro detekci N_2O v oblasti ≈ 4,5–4,6 µm musí řešit potenciální interference s absorpčními pásmy dalších atmosférických plynů. Analýza spektrálních charakteristik pomocí nástroje Spectraplot odhaluje klíčové interakce zobrazené na obrázku 4.



Obrázek 4 Simulovaná absorpční spektra N_2O, CO a CO_2 v infračervené oblasti 4,5-4,6 μm

Vhodnou volbou optického filtru s úzkou propustností 2195–2220 cm^{-1} (4,50–4,56 μm), který maximalizuje selektivitu pro N_2O při zachování dostatečné citlivosti. Toto řešení potlačuje vliv CO_2 (jehož hlavní pásmo leží při 2349 cm^{-1}) a CO (2143 cm^{-1}), jejichž zbytková interference bude kompenzována algoritmicky pomocí korekčních faktorů odvozených z laboratorních kalibrací.

Požadované řešení splňuje předkalibrovaný NDIR senzor $FLOW^{EVO}$ od společnosti smartGAS Mikrosensorik GmbH (Obrázek 5) určený pro detekci oxidu dusného (N_2O) v koncentracích do 500 ppm. Senzor je ideální pro přesnou detekci N_2O v laboratorních, průmyslových i environmentálních aplikacích, kdy jeho rozsah je 0–500 ppm s digitálním rozlišením 1 ppm [9].



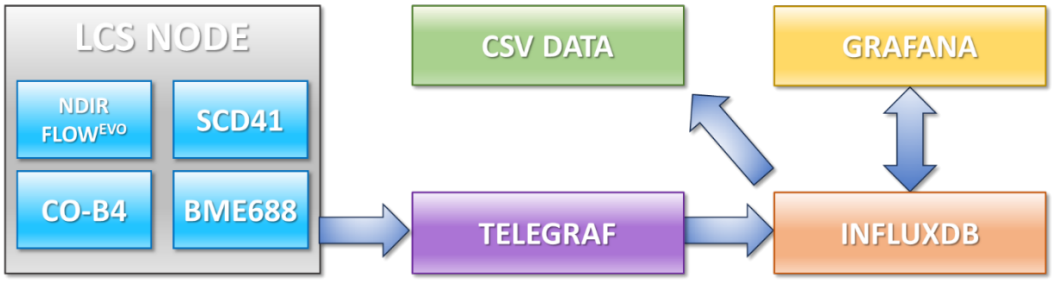
Obrázek 5 Senzor $FLOW^{EVO}$ od firmy smartGAS [9]

V reálných podmínkách s typickými atmosférickými koncentracemi N_2O (≈320 ppb) a CO_2 (≈415 ppm) představuje interference CO_2 <8 % celkového signálu. Při smogových epizodách s koncentracemi, CO až 5 ppm zůstává chyba měření pod 3 %, což potvrzuje účinnost implementovaných kompenzačních mechanismů. Účinnost tohoto přístupu lze dále zvýšit za pomocí současného měření koncentrací CO_2 a CO jinými dostupnými senzory (Sensirion SCD41 a Alphasense CO-B4) a požití vhodných algoritmů.

Takto koncipovaný systém pak umožňuje detekci zvýšených koncentrací N_2O (>1 ppm) spojených s:

- Tepelným rozkladem dusičnanu amonného
- Lesními požáry (korelace s VOC)
- Průmyslovými úniky (chemická výroba, spalovací procesy)

Klíčovým aspektem navrhovaného monitorovacího systému je jeho schopnost kontinuálního sběru dat a jejich okamžitého přenosu do centrálního úložiště. Tato funkcionalita je realizována prostřednictvím integrace NDIR senzoru a dalších s modulem internetu věcí (IoT) založeného na platformě ESP32, který zajišťuje konektivitu a zpracování dat. Toto řešení nazýváme low cost sensor node (LCS node). Schématický rámec pro záznam dat je pak zobrazen na obrázku 6



Obrázek 6 Schematické znázornění rámce pro záznam dat [10]

Naměřená data ze senzorového uzlu jsou přenášena prostřednictvím protokolu MQTT do cloudové infrastruktury. Pro přenos dat je využíván nástroj Mosquitto MQTT broker, který zajišťuje efektivní publikaci dat do specifikovaných témat. Další zpracování dat probíhá v nástroji Telegraf, který transformuje a validuje přijaté informace. Telegraf ukládá data do časové databáze InfluxDB, která je optimalizována pro ukládání časových řad a umožňuje dlouhodobou retenci dat s pokročilými kompresními algoritmy. Vizualizace dat je realizována prostřednictvím platformy Grafana, která poskytuje uživatelsky přívětivé dashboardy pro sledování koncentrací N_2O, CO_2 a dalších parametrů v reálném čase. Grafana také umožňuje nastavení alarmových funkcí při detekci nadlimitních hodnot koncentrací plynů. [10] Vybraná data jsou pravidelně exportována ve formátu CSV, což umožňuje jejich další analýzu a integraci s externími výzkumnými platformami. Tento systém poskytuje robustní řešení pro kontinuální monitoring emisí N_2O v terénních podmínkách, přičemž jeho flexibilita umožňuje škálování až na stovky senzorových uzlů v rámci jedné infrastruktury.

4 ZÁVĚR

Závěr této studie potvrzuje význam monitorování emisí oxidu dusného (N_2O), který je nejen významným skleníkovým plynem, ale i faktorem

poškozujícím ozonovou vrstvu. Vzhledem k jeho dlouhé životnosti v atmosféře a reaktivitě ve stratosféře je důležité sledovat jeho koncentrace z různých zdrojů, jako jsou zemědělství, průmyslové procesy a spalovací procesy. Tento výzkum ukázal, že NDIR technologie představuje efektivní nástroj pro detekci N_2O, který, i když poskytuje nižší spektrální rozlišení než kvantově-kaskádové lasery (QCL), nabízí dostatečnou selektivitu při správné volbě optických filtrů a detekčních parametrů. Experimenty ukázaly, že interference CO_2 při typických atmosférických koncentracích N_2O (≈320 ppb) a CO_2 (≈415 ppm) je menší než 8 % celkového signálu, a při smogových epizodách, kde koncentrace CO dosahují až 5 ppm, zůstává chyba měření pod 3 %. Tyto výsledky potvrzují efektivnost implementovaných kompenzačních mechanismů, které lze dále vylepšit kombinovaným měřením koncentrací CO_2 a CO pomocí dalších dostupných senzorů a vhodných algoritmů. Navrhovaný monitorovací systém, integrovaný s NDIR senzorem a IoT platformou ESP32, umožňuje kontinuální sběr a přenos dat do centrálního úložiště, což zajišťuje efektivní monitorování emisí N_2O. Tento přístup poskytuje flexibilní a nízkonákladové řešení pro dlouhodobé monitorování emisí N_2O v různých aplikacích, od environmentálního monitoringu po průmyslovou bezpečnost. Systém má potenciál přispět k lepšímu porozumění emisním tokům N_2O a podpořit efektivní strategie pro mitigaci jeho emisí.

LITERATURA

[1] HORBAJ, P. Vznik oxidov dusíka a ich vplyv na rozpad ozónovej vrstvy. Chemické listy, 1997, 91.10: 833-839.

[2] ROSSER, W. A.; INAMI, S. H.; WISE, H. The kinetics of decomposition of liquid ammonium nitrate. The Journal of Physical Chemistry, 1963, 67(9), s. 1753-1757.

[3] BERTAGNI, M. B., et al. Minimizing the impacts of the ammonia economy on the nitrogen cycle and climate. Proceedings of the National Academy of Sciences, 2023, 120(46), e2311728120.

[4] BANDARA, K. M. T. S., et al. A low-cost NDIR-based N_2O gas detection device for agricultural soils: Assembly, calibration model validation, and laboratory testing. Sensors, 2021, 21(4), s. 1189.

[5] RICAUD, P., et al. The monitoring nitrous oxide sources (MIN_2OS) satellite project. Remote Sensing of Environment, 2021, 266, s. 112688.

[6] DOSTÁL, M. Mikro/nanomechanické senzory pro monitorování atmosférických škodlivin. Online, Disertační práce. Ostrava: Vysoká škola báňská – Technická univerzita Ostrava, 2021. Dostupné z: http://hdl.handle.net/10084/151349.

[7] HLOUŠKOVÁ, L. Detekce plynů jako prvek technické bezpečnosti osob a majetku. Online, Diplomová práce. Ostrava: Vysoká škola báňská – Technická univerzita Ostrava, 2016. Dostupné z: http://hdl.handle.net/10084/114250.

[8] ROTHMAN, L. S., I. E. GORDON, Y. BABIKOV, A. BARBE, D. CHRIS BENNER, P. F. BERNATH, M. BIRK, L. BIZZOCCHI, V. BOUDON, L. R.

BROWN, A. CAMPARGUE, K. CHANCE, E. A. COHEN, L. H. COUDERT, V. M. DEVI, B. J. DROUIN, A. FAYT, J. M. FLAUD, R. R. GAMACHE, J. J. HARRISON, J. M. HARTMANN, C. HILL, J. T. HODGES, D. JACQUEMART, A. JOLLY, J. LAMOUROUX, R. J. LE ROY, G. LI, D. A. LONG, O. M. LYULIN, C. J. MACKIE, S. T. MASSIE, S. MIKHAILENKO, H. S.P. MÜLLER, O. V. NAUMENKO, A. V. NIKITIN, J. ORPHAL, V. PEREVALOV, A. PERRIN, E. R. POLOVTSEVA, C. RICHARD, M. A.H. SMITH, E. STARIKOVA, K. SUNG, S. TASHKUN, J. TENNYSON, G. C. TOON, VI G. TYUTEREV a G. WAGNER. The HITRAN2012 molecular spectroscopic database. Journal of Quantitative Spectroscopy and Radiative Transfer [online]. 2013, 130, 4–50. ISSN 00224073. Dostupné z: doi:10.1016/j.jqsrt.2013.07.002

[9] SMARTGAS Mikrosensorik GmbH. FLOWEVO Sensor N_2O 500 ppm – Datasheet. Německo: smartGAS Mikrosensorik GmbH, 2023.

[10] Nevrlý, V., Dostál, M., Bitala, P., Klečka, V., Sléžka, J., Polách, P., Nevrlá, K., Barabášová, M., Langová, R., Bernatíková, Š., Martiníková, B., Vašinek, M., Nevrlý, A., Lazecký, M., Suchánek, J., Chaloupecká, H., Kiča, D., & Wild, J. (2024). Varying Performance of Low-Cost Sensors During Seasonal Smog Events in Moravian-Silesian Region. Atmosphere, *15*(11), 1326. https://doi.org/10.3390/atmos15111326

EXPERIMENTÁLNE OVERENIE SORPCIE VYBRANÝCH LÁTOK ZA POUŽITIA SORPČNYCH MATERIÁLOV

Dušan Bóna[1], Iveta Marková[1], Jozef Svetlík[1]

ABSTRAKT

Článok pojednáva o téme sorpčných materiálov na teoretickej a praktickej úrovni. Úvodná kapitola je venovaná teoretickej analýze problému. Zostávajúce kapitoly sa zaoberajú špecifickými sorpčnými materiálmi a výsledkami získanými pri ich testovaní. Testovanie bolo zamerané na motorový olej, pretože takmer pri každej dopravnej nehode vidíme únik motorového oleja.

Kľúčové slová:
Sorpcia, sorpčné materiály, nebezpečné látky, sorpčná kapacita

ABSTRACT

The article discusses the topic of sorption materials on a theoretical and practical level. The introductory chapter is devoted to the theoretical analysis of the issue. The remaining chapters deal with specific sorbent materials and the results obtained in their testing. Testing was aimed on engine oil because almost in every car crash we can see engine oil leak.

Key words:
Sorption, sorption materials, dangerous substances, sorption capacity

1 ÚVOD

Sorpčné materiály sú nevyhnutnou súčasťou vybavenia príslušníkov hasičského a záchranného zboru Slovenskej republiky. Používajú sa vo väčšine prípadov, ako sú dopravné nehody alebo dopravné nehody vozidiel prepravujúcich nebezpečné látky. V súčasnosti je cestná doprava na veľmi vysokej úrovni a počet automobilov stále rastie. Z tohto dôvodu sa zvyšuje aj počet dopravných nehôd, a tak sa objaví mnoho mimoriadnych udalostí, v ktorých je potrebné používať sorpčné materiály [1]. Vzhľadom na polohu Slovenska v centre strednej Európy, je cez naše územie prepravované veľké množstvo materiálov a často hovoríme práve o látkach nebezpečných pre životné prostredie.

1 Ing. Dušan Bóna 1. mája 32, 01026 Žilina, Slovensko, bona1@uniza.sk

Sorpčné materiály sú najúčinnejším prostriedkom na likvidáciu únikov nebezpečných látok, zároveň sú najlepšou ochranou životného prostredia, ak dôjde k úniku nebezpečnej látky [2].

2 ANALÝZA RIEŠENEJ PROBLEMATIKY

Termín sorbent označuje skupinu prevažne pevných látok, ktoré majú schopnosť viazať kvapalné a plynné látky vo svojej štruktúre alebo na svojom povrchu [3]. Sorpcia je proces, pri ktorom sú molekuly z plynných alebo kvapalných látok zachytávané pevným materiálom. Tento proces môže prebiehať dvoma rôznymi spôsobmi, a preto pojem sorpcia zahŕňa dva odlišné javy. Prvým je difúzia molekúl do vnútornej štruktúry pevného materiálu, známeho ako absorbent – tento proces sa nazýva absorpcia. Druhý jav nastáva, keď sa molekuly z plynu alebo kvapaliny hromadia na povrchu pevnej látky – tento proces sa nazýva adsorpcia. Tieto dva procesy často prebiehajú súčasne a sú spoločne označované ako sorpcia, aj keď sa jednotlivo klasifikujú ako absorpcia alebo adsorpcia. Táto dvojaká povaha často vedie k zámene medzi pojmami absorbent a adsorbent [4].

3 EXPERIMENTÁLNE VZORKY

Celkovo bolo použitých 6 vzoriek sorpčných materiálov, ktoré boli testované na dvoch druhoch nebezpečných látok. Testovanie prebehlo na motorovom oleji a na použitom motorovom oleji.

3.1 VAPEX

Vapex má šedo-bielu farbu (obrázok 4.1). Veľkosť zŕn je 0,8 – 2,0 mm a hodnota pH je stanovená v rozmedzí 7 – 9. Výrobca stanovil sorpčnú kapacitu na 18,1. Vďaka jeho hydrofóbnej úprave dokáže plávať na vodnej hladine. Tento sorbent je pomerne prašný a preto je pri jeho používaní potrebné chrániť dýchacie cesty, prípadne ak je to možné zabezpečiť odvetrávanie prachu z prostredia [5].

Obrázok 1 Vapex

Najčastejšie je v HaZz používaný na sorpciu ropných látok, či už na pevnom povrchu alebo dočasne v stojatých vodách. Nakoľko sa jedná o nehorľavú látku tak je možné ho použiť aj pri nehodách s možným rizikom požiaru [5].

3.2 EXPANDOVANÝ PERLIT

Expandovaný perlit je ľahký porézny materiál sivobielej farby, ktorý je vysoko prašný. Je chemicky neutrálny, má nízku špecifickú hmotnosť, je odolný voči plesniam a chemickým mikroorganizmom, má nízku hydroskopiu a je bez zápachu [6].

Obrázok 2 Expandovaný perlit

Najúčinnejší je pri sorpcii kvapalín hydrofóbnej povahy hlavne ropných produktov. Je možné ho použiť na pevnom povrchu a dočasne aj v stojatých vodách. Taktiež slúži na dočisťovanie uniknutých látok z ťažko prístupných priestorov [6].

3.3 JOSYP

Josyp je neprašný, pórovitý a granulovaný. Po nasýtení ostáva tvrdý a je odolný voči pokĺznutiu. Tento sorbent nebol poskytnutý s kartou bezpečnostných údajov a neboli sme ani schopný ju získať, preto tak bol použitý len ako doplnková vzorka. Hlavným dôvodom jeho použitia bola podobnosť so vzorkami akra-sorb a eco-dry plus. Jediným rozdielom bola veľkosť zŕn a tak sme chceli vedieť ako tento parameter ovplyvní výsledky pokusov [7].

Obrázok 3 Josyp

3.4 ECO-DRY PLUS

Eco-dry je pórovitá, neprašná, kremičitá, granulovaná sorpčná drvina. Po nasýtený ostáva tvrdá a je odolná voči pokĺznutiu. Jeho pH je stanovené na 5 – 8 a sorpčná kapacita je 13. Za žiadnych okolností sa nemôže používať v kombinácii s kyselinou fluorovodíkovou. Je možné ho použiť pri vodných aj organických roztokoch a všetkých druhoch olejov. Používať sa môže iba na pevnom povrchu [8].

Obrázok 4 Eco-dry plus

3.5 LITE DRI

Lite-dri je vysoko sorpčná drvina bez abrazívnych účinkov, neprašná a v hydrofóbnej úprave. Používa sa predovšetkým pri odstraňovaní ropných produktov z pevných povrchov alebo aj z vodnej hladiny. Sorpčná kapacita tohto sorbentu je 28 [9].

Obrázok 5 Lite dri

3.6 SORB$_{XT}$

Sorbxt je tvorený zo stopercentne organických sedimentov, ide teda o čistú rašelinu. Má hnedú farbu. Jeho štruktúra nie je jednotná nakoľko je zväčša sýpka ale nachádzajú sa tu aj časti dreva. Sorpčná kapacita je stanovená na hodnotu 27. Zaraďuje sa medzi prírodné sorbenty, ktoré možno nájsť v teréne a použiť ich ako improvizačný prostriedok. Keďže ide o prírodný materiál tak látky viaže na báze uhľovodíkov a je biologicky odbúrateľný. Pri porovnaní s rašelinou ide o totožné látky, jediný rozdiel je v tom, že Sorbxt je viacej podrvený a obsahuje menej dreva [10].

Obrázok 6 Sorb$_{xt}$

4 EXPERIMENTÁLNY POSTUP

Určite jednotnú hmotnosť vzoriek pre každý sorbent, pričom minimálna možná hmotnosť vzorky je 4 g. Hodnotu si zaznamenajte, aby ste predišli chybám. Pripravte zvolenú nebezpečnú látku v kadičke tak, aby jej hladina mala minimálne výšku 2,5 cm. Odváženú vzorku sorbentu nasypte do pripravenej nebezpečnej látky a nechajte pôsobiť 15 minút (± 20 sekúnd).

Po uplynutí 15 minút nalejte roztok na pripravený filtračný papier, ktorý je umiestnený na kovovej mriežke. Nechajte sorbent na filtračnom papieri, kým z

neho neprestane odkvapkávať absorbovaná látka. Po ukončení absorpcie odvážte hmotnosť nasýteného sorbentu spolu s filtračným papierom. Získané hodnoty si zaznamenajte. Postup zopakujte pre všetky vzorky 5krát. Použitý postup vychádza zo štandardu ASTM F726-17 [11].

5 VÝSLEDKY A DISKUSIA

Z hodnôt uvedených v tabuľke 1 môžeme povedať, že perlit má najlepšiu sorpčnú kapacitu na sorpciu oleja. Na druhej strane, najslabšie hodnoty boli zaznamenané pri sorbente Eco-dry.

Tabuľka 1 sorpčné kapacity pre čerstvý motorový olej

Čerstvý motorový olej	Hmotnosť suchej vzorky [g]	Hmotnosť zmáčanej vzorky [g]	Množstvo prijatej látky [g]	Sorpčná kapacita	Sorpčná kapacita [%]
Vapex	5	26,9	21,9	5,38	438
Sorbxt	5	27,2	22,2	5,44	444
Eco-dry	5	11,4	6,4	2,28	128
Lite-dri	5	16,5	11,5	3,3	230
Josyp	5	11,5	6,5	2,3	130
Perlit	5	27,8	22,8	5,56	456

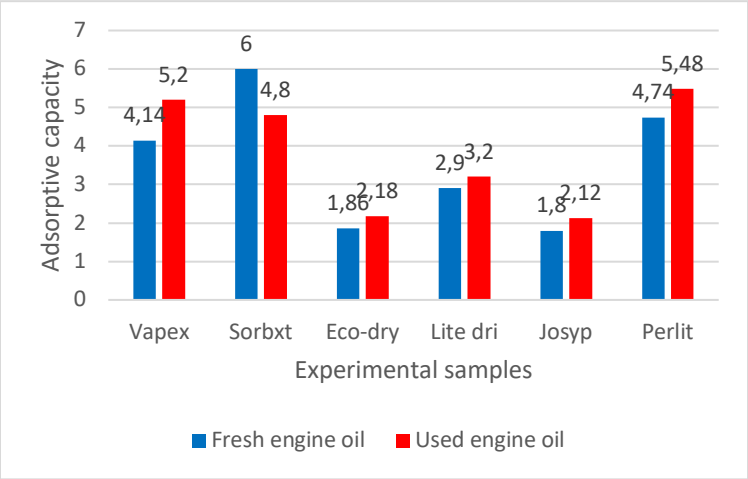
Z hodnôt v tabuľke 1 môžeme vidieť, že najvyššie hodnoty adsorpcie motorového oleja boli zaznamenané pri perlíte, ktorý absorboval 22,8 ml oleja na 5 g svojej hmotnosti. To zodpovedá 456 % jeho pôvodnej hmotnosti. Najnižšia hodnota adsorpcie motorového oleja bola zaznamenaná pri sorbente Eco-dry Plus, ktorý dokázal absorbovať 6,4 ml motorového oleja na 5 g hmotnosti, čím zvýšil svoju hmotnosť o 128 %. Pri pohľade na tabuľku 1 je zrejmé, že najlepšie sorbenty na adsorpciu motorového oleja sú Perlit, Vapex a Sorbxt, keďže ich hmotnosť sa zvýšila o viac ako 400 %.

Z hodnôt v tabuľke 2 môžeme vidieť, že najlepšie hodnoty adsorpcie použitého motorového oleja boli zaznamenané pri sorbente Sorbxt. Dá sa povedať, že rašelina by vykazovala veľmi podobné hodnoty, keďže Sorbxt je z 99 % tvorený rašelinou. Najnižšia hodnota bola zaznamenaná pri sorbente Josyp.

Tabuľka 2 sorpčné kapacity pre použitý motorový olej

Použitý motorový olej	Hmotnosť suchej vzorky [g]	Hmotnosť zmáčanej vzorky [g]	Množstvo prijatej látky [g]	Sorpčná kapacita	Sorpčná kapacita [%]
Vapex	5	26,9	21,9	5,38	438
Sorbxt	5	27,2	22,2	5,44	444
Eco-dry	5	11,4	6,4	2,28	128
Lite-dri	5	16,5	11,5	3,3	230
Josyp	5	11,5	6,5	2,3	130
Perlit	5	27,8	22,8	5,56	456

Z hodnôt zaznamenaných v tabuľke 2 môžeme usúdiť, že najlepším sorpčným materiálom na absorpciu použitého motorového oleja je Sorbxt. Jeho hmotnosť sa zvýšila o 560 % a absorboval 28 ml nebezpečnej látky na 5 g svojej hmotnosti. Najslabším sorpčným materiálom sa ukázal byť Josyp – jeho hmotnosť sa zvýšila len o 90 % a absorboval 4,5 ml použitého motorového oleja na 5 g.



Obrázok 7 Graf porovnania sorpčných kapacít

Na obrázku 7 môžeme vidieť porovnanie sorpčných kapacít pre čerstvý a použitý motorový olej. Zaujímavým zistením z tohto obrázka je, že všetky sorpčné materiály majú nižšiu adsorpčnú kapacitu pre použitý motorový olej. Výnimkou je však Sorbxt, ktorý sa správa opačne – hoci pri čerstvom oleji nedosiahol najlepšie výsledky, pri použitom oleji dosiahol najvyššiu účinnosť.

POĎAKOVANIE

Tento článok bol podporený projektom 041ŽU-4/2023, Vzdelávací a výcvikový modul rozširujúci znalosti, zručnosti a kompetencie študentov programu záchranné služby

LITERATÚRA

[1] Marková, I., 2009. Ekologické prostriedky na zachytávanie nebezpečných látok uniknutých v dôsledku dopravnej nehody. In: Súčinnosť záchranných zložiek integrovaného záchranného systému pri dopravných nehodách na pozemných komunikáciach, Žilina, s. 8.
[2] Marková, I., 2006. Sorbenty – prostriedky používané pri zachytávaní uniknutej nebezpečnej látky na vodnej hladine. In: Riešenie krízových situácií pri úniku nebezpečnej látky na vodných hladinách, Zvolen, s. 41-50.
[3] Shunguang, D., 2006. Sorbent technology. Research gate.
[4] Marková, I., 2003. Ekologické prostriedky pre likvidáciu unikajúcich látok pri zásahu hasičov. In: Riešenie krízových situácií v špecifickom prostredí, Žilina, s. 311- 317.
[5] Akra sorb, 2021. Karta bezpečnostných údajov Vapex.
[6] Akra sorb, 2021. Karta bezpečnostných údajov Expandovaný perlit.

[7] Akra sorb, 2021. Karta bezpečnostných údajov Josyp.
[8] Akra sorb, 2021. Karta bezpečnostných údajov Eco-dry.
[9] Akra sorb, 2021. Karta bezpečnostných údajov Lite dri.
[10]Akra sorb, 2021. Karta bezpečnostných údajov $Sorb_{xt}$.
[11] Štandardná testovacia metóda ASTM F726-17

POŽIARNA BEZPEČNOSŤ EKOLOGICKÝCH IZOLAČNÝCH MATERIÁLOV: SKÚMANIE ICH VLASTNOSTÍ A DEGRADÁCIE

Dávid Boráros[1], Stanislava Gašpercová[2]

ABSTRAKT

Tento projekt sa zameriava na skúmanie vlastností recyklovaných a prírodných tepelnoizolačných materiálov s dôrazom na ich tepelnú degradáciu a požiarne správanie. V súčasnosti je ekologické stavebníctvo čoraz populárnejšie, pričom udržateľné izolačné materiály zohrávajú kľúčovú úlohu pri znižovaní energetickej náročnosti budov. Cieľom výskumu je analyzovať, ako sa tieto materiály správajú pri vystavení zvýšeným teplotám a sálavému teplu, a určiť, do akej miery dochádza k ich degradácii, strate izolačných vlastností či zvýšeniu horľavosti. Výsledky tejto štúdie poskytujú cenné údaje pre ďalší vývoj ekologických izolácií s lepšími tepelnými a protipožiarnymi vlastnosťami.

Kľúčové slová:
ekologické izolačné materiály, sálavé teplo, tepelná degradácia, požiarna bezpečnosť.

ABSTRACT

This project focuses on the study of recycled and natural thermal insulation materials, emphasizing their thermal degradation and fire behavior. Nowadays, ecological construction is becoming increasingly popular, with sustainable insulation materials playing a key role in reducing the energy demand of buildings. The aim of this research is to analyze how these materials behave when exposed to elevated temperatures and radiant heat, determining the extent of their degradation, loss of insulating properties, or increased flammability. The results of this study will provide valuable data for the further development of ecological insulation materials with improved thermal and fire-resistant properties.

Key words:
ecological insulation materials, radiant heat, thermal degradation, fire safety.

1 Ing. Dávid Boráros[1], Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, ul. 1. mája 32, 010 01 Žilina, +421/907344190, boraros12@gmail.com
2 doc. Bc. Ing. Stanislava Gašpercová, PhD.[1], Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, ul. 1. mája 32, 010 01 Žilina, 041/5136796, stanislava.gaspercova@uniza.sk

ÚVOD

Požiare sa v rôznych budovách na Slovensku vyskytujú pomerne často, preto je protipožiarna ochrana stavebných materiálov dôležitou a aktuálnou témou. Pri výstavbe nových budov musia byť splnené aj požiadavky na protipožiarnu ochranu. Poznanie protipožiarnych vlastností použitých materiálov a uplatnenie vhodnej inštalačnej technológie sú mimoriadne dôležité v praxi protipožiarnej ochrany. Jedným z významných aspektov pri výstavbe nových budov je zabezpečenie ich tepelnej izolácie, pričom sa čoraz viac využívajú ekologické izolačné materiály. Medzi často používané tepelnoizolačné materiály patria aj recyklované textilné izolácie a drevovláknité dosky, ktorých inštalácia musí byť vykonaná v súlade s osobitnými normami. Tieto materiály väčšinou sú použité ako vnútorné tepelné izolácie. Kvôli tomu sú veľmi nebezpečné lebo pri horení produkujú značné množstvo toxických splodín, ktoré výrazne ohrozujú osoby v zasiahnutom priestore.

Cieľom výskumu je skúmať zmeny v textilných a drevovláknitých izolačných materiáloch v dôsledku priameho pôsobenia tepla v laboratórnom prostredí. Výsledky meraní môžu prispieť k plánovaniu budúcich výskumných úloh.

1 LABORATÓRNE MERANIE

Štandardné testy sa väčšinou zameriavajú na skúmanie horľavosti a požiarnych vlastností materiálov pri plameni, preto bol vykonaný odlišný laboratórny experiment na skúmanie nárastu teploty a úbytku hmotnosti týchto materiálov. V odbornej literatúre možno nájsť niekoľko príkladov skúmania správania recyklovaných textilných izolácií a drevovláknitých materiálov pri pôsobení plameňa. Použité však boli rôzne odlišné meracie zariadenia a metódy a skúmané boli rôzne javy ako sú napríklad vplyv vlhkosti alebo vplyv hustoty alebo hrúbky materiálu, atď. [1-3].

V experimente prezentovanom v tejto práci je možné presne nastaviť teplotu tepelného zdroja a presne merať sálavé teplo dopadajúce na povrch vzoriek, čím sa dá efektívne detegovať vnútorná zmena teploty týchto materiálov. Pred začiatkom laboratórnych meraní boli skúmané požiarno-bezpečnostné vlastnosti vybraných materiálov.

Pri výrobe tepelnoizolačných materiálov z recyklovaného textilu sa textilný odpad najprv rozvlákňuje, čistí a mieša s retardérmi horenia, ako sú fosfátové alebo boritanové zlúčeniny. Následne sa materiál lisuje do izolačných dosiek alebo spracováva do voľnej vláknitej formy určenej na fúkanú izoláciu. Pri vystavení vysokým teplotám môžu tieto materiály uvoľňovať toxické plyny, ako sú CO (oxid uhoľnatý), CO_2 (oxid uhličitý), HCN (kyanovodík) alebo NO (oxidy dusíka), najmä ak obsahujú syntetické vlákna alebo zvyškové chemikálie z textilného priemyslu.

Drevovláknité izolačné materiály sa vyrábajú z drevenej hmoty, ktorá sa rozvlákňuje, suší a mieša s vodou alebo prírodnými spojivami, ako sú lignín alebo škrob. Po lisovaní a sušení vznikajú izolačné dosky rôznej hustoty. Pri

vyšších teplotách (nad +80 ºC) dochádza k degradácii lignocelulózových vlákien, čo vedie k úbytku pevnosti a rozmerovej stability materiálu. Pri horení sa uvoľňujú plyny ako CO, CO_2, formaldehyd, fenoly a ďalšie prchavé organické zlúčeniny, ktoré môžu predstavovať riziko pre zdravie osôb v zasiahnutom priestore [4-6].

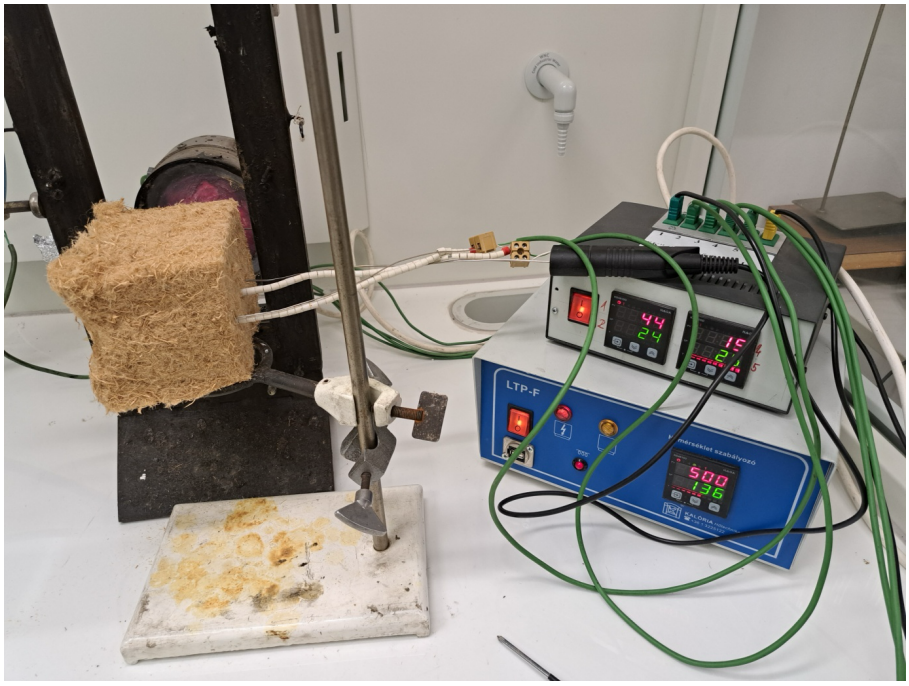
Z tohto dôvodu sa recyklované textilné a drevovláknité izolácie neodporúčajú používať na miestach trvalo vystavených vysokým teplotám alebo v priestoroch s vysokým rizikom požiaru. Tepelné vlastnosti týchto materiálov sú zhrnuté v tabuľke 1.

Tabuľka 1 Tepelné vlastnosti materiálov (autor)

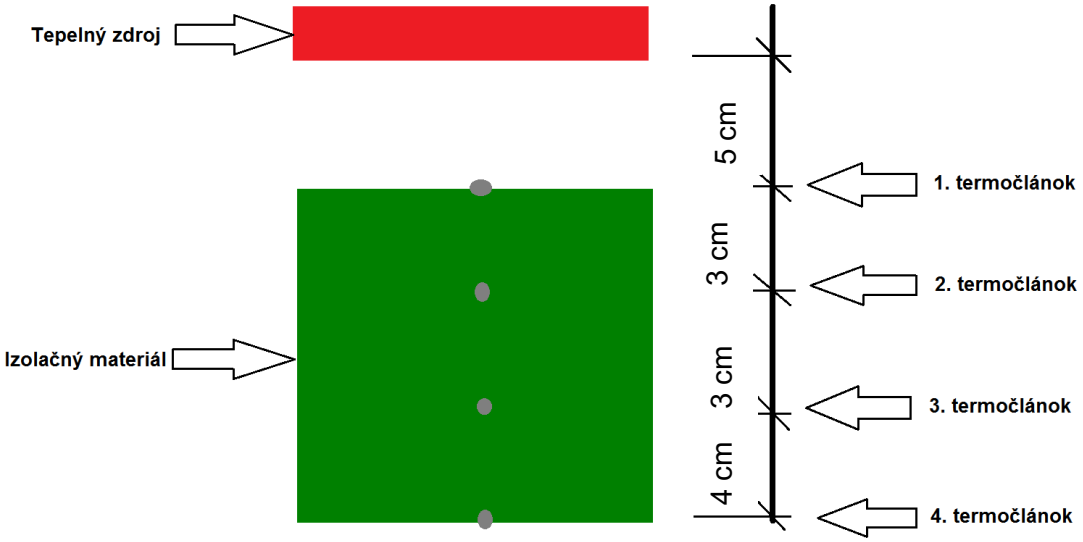
	Hustota [kg/m^3]	Súčiniteľ tepelnej vodivosti [W/(m*K)]	Merná tepelná kapacita [J/(kg*K)]	Faktor difúzneho odporu [-]	Trieda reakcie na oheň [-]
Textilná izolácia	24	0,036	1500	1,65	E
Drevovláknitá izolácia	60	0,036	2100	0,5	E

1.1 PRIEBEH MERANIA

Merania boli vykonané s nastaviteľným zdrojom tepla, pričom tepelné senzory boli umiestnené pred ním a v testovanom vzorku a dáta boli zaznamenané pomocou štvorkanálového dátového záznamníka. Výsledky merania boli uložené do počítača pripojeného k zariadeniu. Meracie zariadenie je znázornené na obr. 1, náčrt merania je znázornený na obr. 2.



Obrázok 1 Meracie zariadenie (autor)



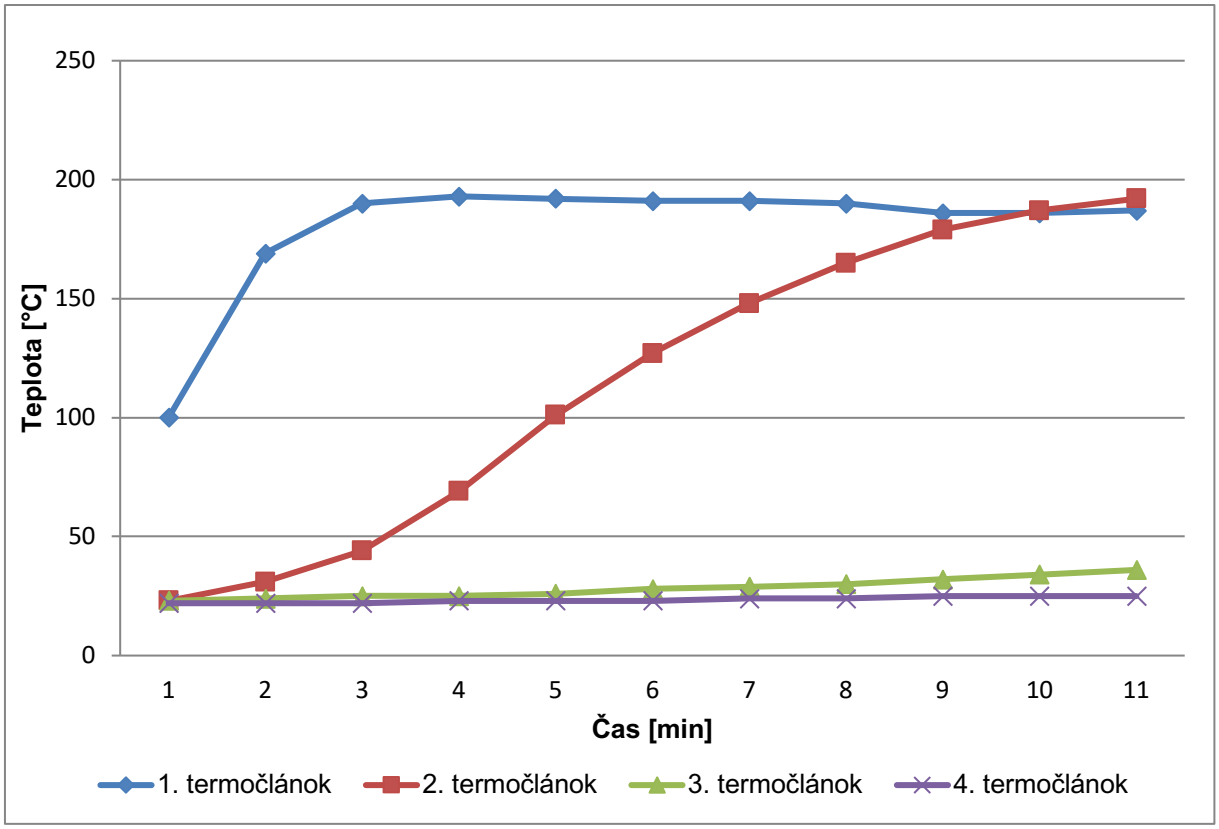
Obrázok 2 Náčrt merania (autor)

Vzorky s jednotnou šírkou 10 x 10 cm a dĺžkou zodpovedajúcou hrúbke materiálu boli pripravené na testovanie. Do každého vzorku boli termočlánky umiestnené v 3 cm odstupoch do hĺbky 5 cm od kraja a vzorka bola následne pripevnená na držiak vo vzdialenosti 5 cm pred zdrojom tepla. Počas meraní bol zdroj tepla nastavený na teplotu 500 ºC. Senzor teploty umiestnený pred vzorkou nameral teplotu 100 ºC v dôsledku vzduchovej medzery medzi zdrojom tepla a vzorkou.

Na začiatku merania bola odstránená tepelnoizolačná vrstva a vzorka bola vystavená sálavému teplu pri teplote 100 ºC počas 10 minút. Počas meraní sa zistilo, že priebežne po 3 až 6 minútach teplota na prvom senzore vo vzorke presiahla 120-140 ºC, čo naznačuje, že v textilných a drevovláknitých vzorkách sa pri teplote 100 ºC začínajú po krátkom čase exotermické procesy.

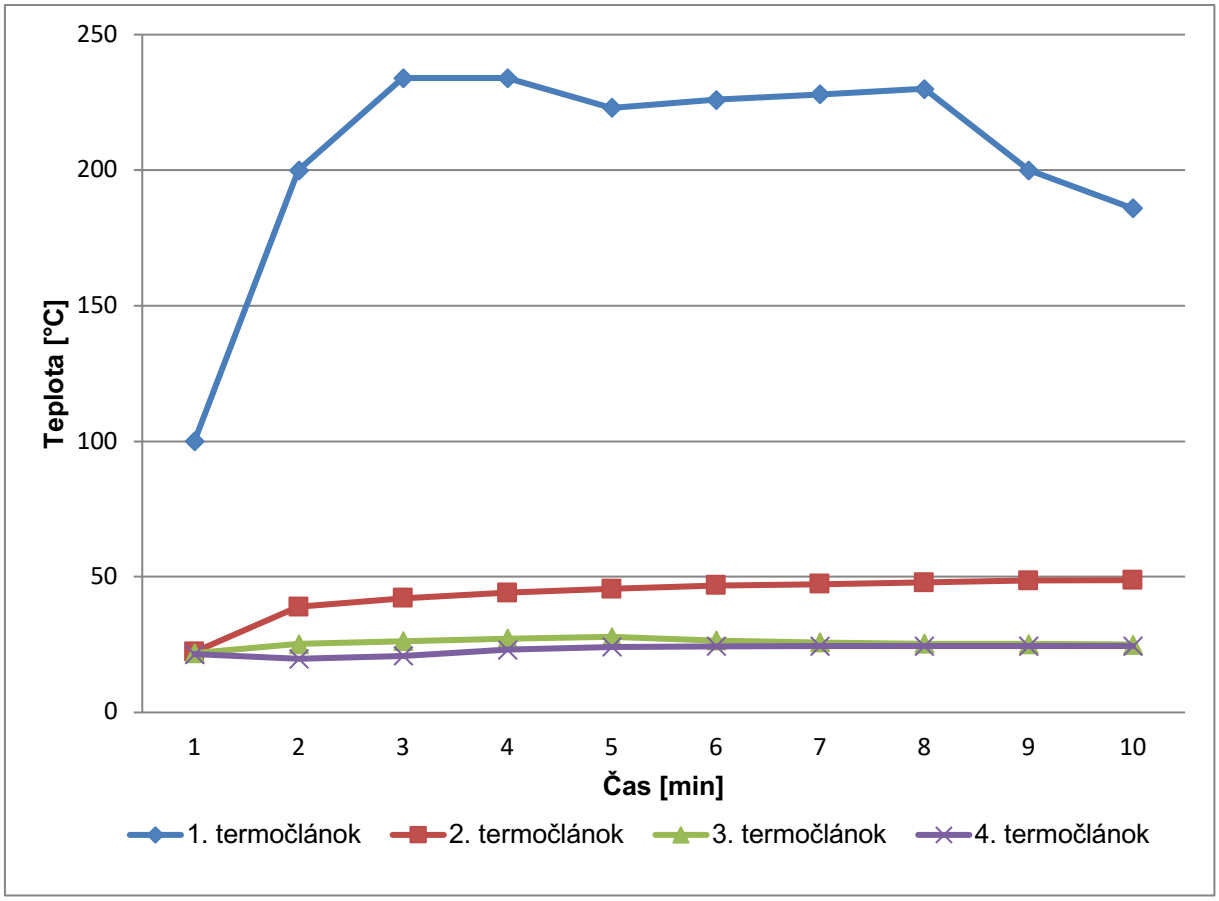
2 INTERPRETÁCIA VÝSLEDKOV

Výsledky meranie sú uvedené na obr. 3-4. Analýzou výsledkov možno konštatovať, že prvý termočlánok zaznamenal prudký nárast teploty, ktorý sa stabilizoval okolo 200 °C a postupne mierne klesal. Druhý termočlánok ukázal postupný a kontinuálny nárast teploty, pričom po 10 minútach sa jeho hodnota vyrovnala s teplotou 1. termočlánku (okolo 200 °C). Tretí a štvrtý termočlánok zaznamenali len mierne zvýšenie teploty (do 40 °C). Počas meraní nedošlo k vzniku plameňov, avšak počas pokusu bolo pozorované slabé dymenie.



Obrázok 3 Výsledky merania vzorky textilného materiálu (autor)

Na základe analýzy výsledkov možno konštatovať, že v drevovláknitom materiáli prvý termočlánok zaznamenal výrazný nárast teploty, pričom už po 2 minútach prekročila 200 °C. Maximálna teplota sa ustálila okolo 230 °C, následne po 8. minúte začala klesať, čo súvisí s degradáciou materiálu, zmenou jeho tepelnej vodivosti a stratou hmotnosti. Druhý termočlánok ukazuje mierne stúpajúcu teplotu, ktorá sa po cca 5. minúte stabilizovala pod 50 °C. Druhý termočlánok zachytáva mierny nárast teploty, čo naznačuje postupné šírenie tepla do materiálu, ale bez prudkého ohrevu. Tretí a štvrtý termočlánok vykazujú len minimálny nárast teploty, pohybujú sa približne na úrovni 20-30 °C a zostávajú stabilné po väčšinu experimentu. Počas meraní nedošlo k vzniku plameňov, avšak počas pokusu bolo pozorované silné dymenie.



Obrázok 4 Výsledky merania vzorky drevovláknitého materiálu (autor)

Textilná izolácia vykazovala rýchly nárast teploty v prvotných vrstvách, pričom už pri teplote 100 °C začali exotermické procesy. Počas testu bolo pozorované mierne dymenie, čo naznačuje rozklad organických zložiek. Drevovláknitá izolácia sa zahrievala rýchlejšie ako textilná, pričom prvý termočlánok zaznamenal teplotu nad 200 °C už po 2 minútach. Materiál sa postupne degradoval, čo sa prejavilo stratou hmotnosti a zvýšeným dymením.

ZÁVER

Výsledky experimentov ukázali, že recyklované textilné a drevovláknité izolačné materiály majú obmedzenú odolnosť voči tepelnému zaťaženiu. Pri vystavení sálavému teplu dochádza k ich degradácii a významnej zmene teplotných charakteristík. V rámci bezpečnostného hodnotenia je možné konštatovať, že tieto ekologické izolačné materiály nie sú vhodné do priestorov s trvalým tepelným namáhaním alebo vysokým rizikom požiaru. Výskum potvrdil potrebu ďalšieho vývoja protipožiarnych úprav a optimalizácie zloženia materiálov s cieľom zvýšiť ich odolnosť voči vysokým teplotám a minimalizovať uvoľňovanie toxických plynov.

LITERATÚRA

[1] MACHNOWSKI, W., WAS-GUBALA, J. 2021. Evaluation of Selected Thermal Changes in Textile Materials Arising in the Wake of the Impact of Heat Radiation. In: Advancing Open Science. Dostupné na internete: <https://www.mdpi.com/2076-3417/11/15/6989>.

[2] MAKOVICKÁ, L., GAŠPERCOVÁ, S. 2017. Stavebné materiály a ich skúšanie pre potreby ochrany pred požiarmi. FBI UNIZA, Žilina. s. 107-115.

[3] MAKOVICKÁ, L., MITRENGA, P., JANCÍK J., TITKO, M., EFHAMISISI, D., KOŠÚTOVÁ, K., 2022. Fire Behaviour of Treated Insulation Fibreboards and Predictions of its Future Development Based on Natural Aging Simulation: Frontiers in Materials. Dostupné na internete: <https://www.frontiersin.org/journals/materials/articles/10.3389/fmats.2022.891167/full>.

[4] ČAJKO, J., 2025. Rozhovor o prírodných tepelnoizolačných materiálov. Tepore s.r.o., Banská Bystrica. Osobná komunikácia [2025-02-14].

[5] FUTRIKANIČ, M., 2025. Rozhovor o textilných tepelnoizolačných materiálov. SK-TEX s.r.o., Bratislava. Osobná komunikácia [2025-02-14].

[6] VAŇKOVÁ, L., 2025. Komunikácia o prírodných tepelnoizolačných materiálov. ECOINSUL s.r.o., [online]. [2025-02-20].

TECHNOLOGICAL AND FIRE SAFETY ASPECTS OF ECOLOGICAL INSULATION MATERIALS PRODUCTION

Dávid Boráros[1], Stanislava Gašpercová[2]

ABSTRACT

This work analyzes the technological and fire safety aspects of producing ecological insulation materials, with a specific focus on recycled textile and wood fiber insulation. The main objective is to identify and evaluate the risks associated with the production of this material using a risk matrix and checklists. The study explores the characteristics of ecological buildings, methods of manufacturing their components, and assesses whether the production of recycled textile and wood fiber insulation falls under processes with a risk of major industrial accidents. The results may contribute to improving the safety and sustainability of the production process.

Key words:
ecological buildings, recycled textile insulation, wood fiber insulation, risk analysis, risk analysis.

INTRODUCTION

Ecological buildings represents a modern approach to sustainable construction characterized by the use of natural, recyclable and environmentally friendly materials. The goal of such buildings is to minimize negative environmental impacts, reduce the carbon footprint and ensure a high level of living comfort.

Non-traditional insulation materials, such as hemp fibers, wood fiber boards and recycled textile insulation are increasingly used in ecological buildings. However, the production processes associated with these materials bring new technological challenges and potential risk. This analysis may contributes to a better understanding of safety aspects in ecological production and help mitigate potential negative impacts on the work environment and surroundings.

1 Ing. Dávid Boráros[1], Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, ul. 1. mája 32, 010 01 Žilina, +421/907344190, boraros12@gmail.com
2 doc. Bc. Ing. Stanislava Gašpercová, PhD.[1], Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, ul. 1. mája 32, 010 01 Žilina, 041/5136796, stanislava.gaspercova@uniza.sk

1 CHARACTERISTICS OF ECOLOGICAL BULDINGS

Ecological construction, also known as sustainable or green building, in an approach to designing and constructing buildings that minimizes negative environmental impacts and maximizes resource efficiently throughout the building's life cycle. Sustainable construction involves minimizing environmental impact and optimizing resource use at all stages of the construction project. This includes using sustainable methods and materials to ensure that building operation and maintenance have minimal long-term environmental impact.

Methods of ecological construction:

- use of renewable and recycled materials,
- reduction of energy demand of the completed building,
- reduction of the energy demand of the completed building,
- reduction of construction waste on-site,
- protection of natural habitats during and after construction.

Ecological buildings must be evaluated and certified according to various standards, such as:

- LEED (Leadership in Energy and Environmental Design) - an international certification system assessing building sustainability,
- BREEAM (Building Research Establishment Environmental Assessment Method) - a European system for evaluating building sustainability,
- Passive House - a standard for extremely energy-efficient buildings [1].

The goal of ecological buildings is to create a healthy and comfortable environment for users while reducing energy, water and material consumption, as well as minimizing waste and harmful emissions. This is achieved through various strategies, such as using environmentally preferred materials and energy-efficient systems like solar panels or natural thermal insulation materials. Natural and recyclable materials such as wood, hemp, straw and textiles are preferred. Using natural or recycled materials reduces construction waste, leading to lower CO_2 emissions and a smaller environmental impact [2].

The implementation of ecological construction brings not only environmental benefits but also economic and social advantages, including reduced operating costs, improved occupant health and the conservation of natural resources for the future. Sustainable construction is an essential part of the future of the building industry, as it helps address climate change, reduce building energy demands and improve people's quality of life. It employs natural and recycled materials, minimizes resource consumption and introduces innovative technologies for sustainable building operation [3].

1.1 PRODUCTION OF COMPOMENTS FOR ECOLOGICAL BUILDINGS

The production of components for ecological buildings involves various environmentally friendly technologies and processes that use renewable or recycled materials. In Slovakia, ecological insulation materials such as wood fiber, hemp insulation, textile insulation and cellulose are predominantly imported from neighboring countries, including Poland, Germany and Austria. The selected component analyzed in this study is internal thermal insulation.

Wood Fiber

Wood fiber boards are ecological insulation materials made from wooden fibers. They are known for their excellent thermal and acoustic insulation properties. Wood fiber insulation naturally insulates floors, walls, ceilings and roofs of buildings. It is particularly suitable for new construction, especially in low-energy and passive houses. Due to its high bulk density and composition, in the event of a fire, it tends to smolder rather than rapidly spread flames.

Wood fibers are obtained from waste wood or sustainably managed forests, mainly spruce and pine. The production process is divided into wet and dry methods. In wet process, wood chips are mixed with water, heated and mechanically defibered. These fibers are then pressed into boards of various thicknesses and densities. The process also involves drying at around 180 ºC and surface treatment. Free fibers are separated in a cyclone and packed separately. Flexible mats are mixed with synthetic textile fibers or resin and dried using hot air or steam. The primary difference between wet and dry processes is that dry methods use adhesives or natural binders instead of water [4].

Fires in drying units used to occur frequently due to older first-generation equipment. However, the risk has been significantly reduced with technological modernization. The production process uses steam and hot air, which may pose safety hazards. Additionally, isocyanate-based resin, which is toxic and potentially carcinogenic, is used in manufacturing. It is stored in specialized bunkers to prevent leaks, and in case of accidental exposure, it reacts with water to neutralize. After its chemical reaction with steam and fibers, it forms polyurethane, which is non-reactive [5].

Hemp

Hemp insulation materials are produced from the fast-growing annual plant Cannabis sativa. These insulation materials are among the most ecological, as they are naturally resistant to mold and pests, have good thermal insulation properties, and are vapor-permeable. Hemp insulation is used in walls, roofs and floors as thermal and acoustic insulation, making it suitable for ecological buildings.

Hemp fibers are obtained from plants grown without pesticides. After harvesting, the hemp stalks are processed into fibers, separating them from the harder parts. The fibers are then combined with BiCo fibers, spun and pressed

into insulation boards or mats. Natural binders and fire-resistant agents are often added during production. Hemp insulation materials are produced exclusively using a dry process [4].

Cellulose

Cellulose insulation is made from recycled paper, primarily newspapers. It is known for its excellent thermal insulation properties and ability to regulate moisture. Cellulose is suitable as thermal and acoustic insulation in all structural cavities, effectively minimizing thermal bridges. It is widely used in low-energy and passive houses.

Recycled paper is ground into fine fibers, which are then treated with natural fire, mold and pest-resistant agents such as borax. The treated cellulose is packed into bags and is ready for application [4].

Textile

Recycled textile material, primarily cotton, is sourced from second-hand clothing, production waste or worn-out workwear. After processing, this material can be used as insulation. These insulation are soft, flexible and have good thermal insulation properties. In Slovakia, approximately 100 000 tons of textile waste are generated annually, which can be processed using the environmentally friendly airlaid method.

The production process occurs exclusively using a dry method. The collected textiles are sorted, cleaned and shredded into fibers. Fire retardants or pest-resistant agents may be added. The fibers are mixed with BiCo fibers for bonding, pressed into insulation mats or boards, dried at temperatures around 120-160 ºC, then cooled and stored [4-6].

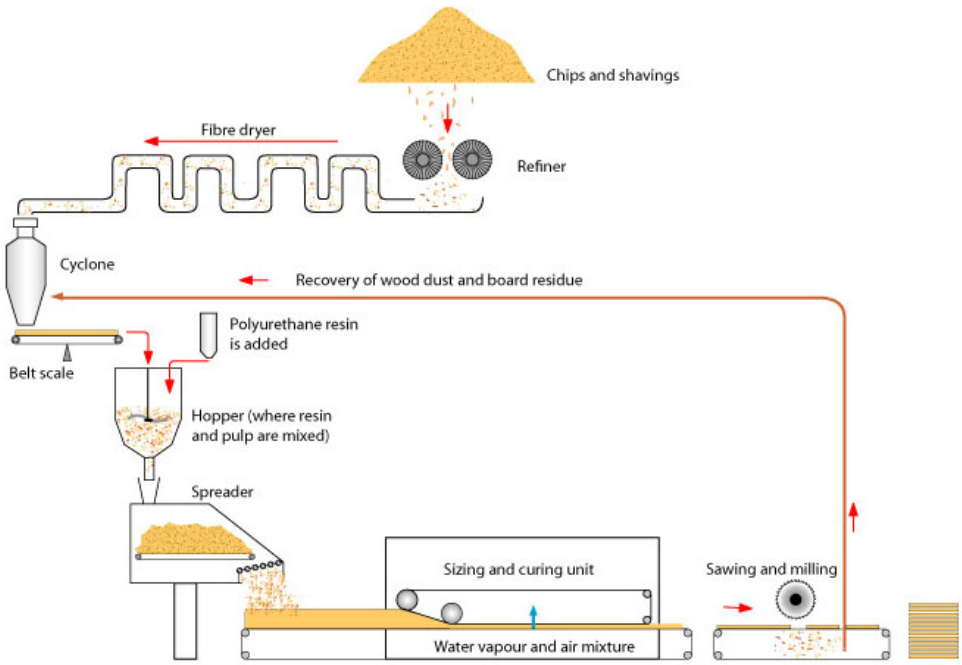


Figure 1 Manufacturing Process of Insulation Material(autor)

2 RISK ANALYSIS OF THE PRODUCTION OF ECOLOGICAL INSULATION MATERIALS - TEXTILE INSULATION MATERIALS

The objective of this section is to conduct a risk analysis of selected technological element. For this purpose, an appropriate identification method will be used to assess potential hazards, their likelihood of occurrence and possible impacts.

In the case of recycled textile insulation materials, we analyze risks in various stages of the production process using the Risk Matrix and Checklist Analysis (CLA):

- collection and sorting of textiles,
- processing and cleaning of fibers,
- mixing with BiCo fibers and pressing,
- drying of insulation mats,
- cooling and storage.

Risk Matrix

This evaluates risks based on the likelihood of occurrence and the severity of consequences.

Table 2.1 Risk Table (autor)

Hazards	Probability (P)	Severity (S)	Risk (PxS)	Measures
Fire caused by an unwanted metal object in the material	High	Critical (possible fire)	**High**	Metal detectors, input material control, cooperation with suppliers on alternative packaging
Fire risk during the drying of insulation mats	Medium	Critical (life-threatening)	**High**	Thermal sensors, fire protection measures, firefighting equipment
Dust generation during textile crushing	Medium	Severe (respiratory issues, flammability)	**Medium**	Ventilation, protective masks, extraction systems
Contact with sharp machine parts during pressing	Medium	Severe (hand injuries)	**Medium**	Protective gloves, safety covers
Electrostatic discharge during fiber handling	Medium	Mild (possible ignition)	**Medium**	Grounding, anti-static measures
Improper storage of material	Low	Mild (possible self-ignition)	**Low**	Proper storage, humidity control

Table 2.2 Risk Matrix (autor)

		High -**3**	Critical -**4**	
Probability of occurrence	High - **3**			**Fire from metal**
	Medium -**2**	**Electrostatic discharge**	**Contact with machine** **Dust from crushing**	**Fire during drying**
	Low -**1**	**Storage/humidity**		
		Mild -**1**	Severe -**2**	Critical -**3**
		Severity of consequences		

CLA: Checklist Method

A large number of control records can be set up for each machine and device. The checklist focuses specifically on fire risk.

Table 2.3 Checklist (autor)

Questions	yes	no
Do you use oxidizing or flammable substances?	x	
Do you store oxidizing or flammable substances in ventilated rooms?	x	
Do you have "Material safety Data Shelter" for all hazardous chemicals used?	x	
Are there sources of ignition or self-ignition?	x	
Are workplaces with fire risks properly marked?	x	
Are employees handling flammable substances regularly trained on the hazards of these substances?	x	
Is fire protection equipment available and adequate?	x	
Are firefighting devices regularly maintained?	x	
Are firefighting devices easily accessible?	x	
Have emergency measures and contingency plans been developed?	x	
Are escape routes and emergency exits marked?	x	
Are fire alarm and extinguishing systems in place?	x	
Are fire drills conducted regularly?	x	
Does the building have a non-combustible structural design?	x	
Have measures been taken to reduce risks?	x	
Is there a storage facility for flammable gases on the premises?		x
Is there a storage facility for flammable liquids on the premises?		x

Is an automatic detection system installed in the building?	x	
If yes, is it installed throughout the entire building?	x	
Are smoke and heat control system devices present in the building?	x	
If yes, are these devices installed throughout the entire building?	x	
Are these devices properly marked?	x	
Has the risk of fire from electrical short circuits been reduced?	x	
Is smoking prohibited throughout the building?	x	
Are measures in place to prevent the use of open flames in the building?	x	
Are there fire closures with panic locks on escape routes?	x	
Is the functionality of panic locks checked regularly?	x	
Are emergency signs visible from any locations?	x	
Are escape routes protected in the building?	x	

Preventive Measures

- proper storage of flammable substances,
- elimination of potential ignition and self-ignition sources,
- equipping workplaces with suitable fire extinguishers,
- ensuring regular inspection of electrical equipment.

3 UNDESIRABLE EVENTS IN THE PRODUCTION PROCESS AND THE THREAT OF MAJOR INDUSTRIAL ACCIDENT

Several undesirable events may occur in the production process, such as fire risks, dust-related hazards, mechanical risks, electrostatic risks and storage-related risks.

Fires may originate from metal objects in the material, such as impurities, screws or wire fragments, which can generate sparks upon contact with machines. Uncontrolled temperatures can lead to overheating and fire. Accumulated fine dust may be explosive or pose respiratory and allergic risks to workers. Mechanical risks include the danger of trapping hands or clothing in pressing or crushing mechanisms and material falling during storage. Electrostatic discharge during fiber handling can generate sparks and ignite fires. Improper storage can increase the risk of self-ignition or the accumulation of hazardous gases.

According to statesments from representatives and employees of affected companies (SK-TEX ltd., TEPORE ltd., ECOINSUL ltd.) that manufacture, store or sell natural insulation materials, these companies **do not fall** enterprises at **risk of major industrial accident**. Based on available information, none of the mentioned companies store or process quantities and types of hazardous substances that would require classification as enterprises with the risk of a major industrial accident [8-11].

CONCLUSION

Based on the conducted analysis, it can be concluded that ecological insulation materials significantly contribute to sustainable construction. However, their production process may involve certain technological and safety risks. The use of risk matrices and checklists enabled the identification of potential hazards and the assessment of their severity in an industrial context. The analysis results indicate that the production of recycled textile insulation does not pose a high risk of major industrial accident. However, it is essential to closely monitor each step of the production process and implement adequate safety measures. Special attention should be given to the handling of chemical additives, dust control and potential fire safety risks.

LIST OF REFERENCES

[1] *Green building.* 2025 [online], [cit. 2025-02-15]. Dostupné na: https://en.wikipedia.org/wiki/Green_building

[2] *Sustainable design.* 2025 [online], [cit. 2025-02-15]. Dostupné na: https://www.gsa.gov/real-estate/design-and construction/sustainability/sustainable design

[3] *Sustainability in Construction.* 2024 [online], [cit. 2025-02-15]. Dostupné na: https://compliancechain.com/sustainability-in-construction-why-it-matters/

[4] ČAJKO, J., 2025. *Rozhovor o prírodných tepelnoizolačných materiáloch*. Tepore s.r.o., Banská Bystrica. Osobná komunikácia [2025-02-14]

[5] RATZOW, H., 2025. *Komunikácia o výrobe prírodných izolačných materiálov.* Naturheld. [online]. henrik.ratzow@naturheld.global. Emailová komunikácia [2025-03-10]

[6] ING. FUTRIKANIČ, M., *Rozhovor o recyklovaných tepelnoizolačných materiáloch.* SK-TEX s.r.o., Bratislava. Osobná komunikácia [2025-02-21]

[7] VAŇKOVÁ, L., *Komunikácia o prírodných tepelnoizolačných materiáloch*. ECOINSUL s.r.o., [online]. lucie.vankova@ecoinsul.eu. Emailová komunikácia [2025-02-20]

[8] *Základy posudzovania rizík.* 2007. Európska agentúra pre bezpečnosť a ochranu zdravia pri práci. [online], [cit. 2025-02-25]. Dostupné na: https://www.ip.gov.sk/wp-content/uploads/2019/10/Zaklady_posudzovania_rizik.pdf

[9] *Posudzovanie vplyvov na životné prostredie.* 2025 [online], [cit. 2025-03-02]. Dostupné na: https://www.enviroportal.sk/eia/detail/zavod-spolocnosti-sk-tex-s-r-o-na-vyrobu-zvukovej-tepelnej-izolacie-za

[10] *Industrial safety.* 2025 [online], [cit. 2025-03-02]. Dostupné na: https://environment.ec.europa.eu/topics/industrial-emissions-and-safety/industrial-accidents_en

[11] *SMERNICA EURÓPSKEHO PARLAMENTU A RADY 2012/18/EÚ zo 4. júla 2012 o kontrole nebezpečenstiev závažných havárií s prítomnosťou nebezpečných látok, ktorou sa mení a dopĺňa a následne zrušuje smernica Rady 96/82/es.* 2012 [online], [cit. 2025-03-02]. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32012L0018

RESILIENT COMPANIES

David Březina[1]

ABSTRAKT

Tento příspěvek se zabývá současnými výzvami v oblasti bezpečnostního managementu a implementací souvisejících strategií. Zdůrazňuje zásadní roli školení zaměstnanců jako klíčové součásti odolnosti organizace. Školení zaměstnanců zvyšuje povědomí, připravenost a schopnost reakce. Zároveň podporuje kulturu odpovědnosti a bezpečnosti uvnitř organizací. Investice do kontinuálního vzdělávání posiluje celkové řízení rizik. Článek tvrdí, že moderní bezpečnostní strategie musí být úzce propojeny s programy školení. Tato synergie zvyšuje schopnost organizace odolávat krizím. Zjištění zdůrazňují, že školení není jen podpůrným prvkem, ale nezbytnou součástí efektivního bezpečnostního managementu.

Kľúčové slová:
Security management, rizika, odolnost, zaměstnanci

ABSTRACT

This contribution explores current challenges in the field of security management and the implementation of related strategies. It emphasizes the vital role of employee training as a key component of organizational resilience. Employee training enhances awareness, preparedness, and response capabilities. It also fosters a culture of responsibility and security within organizations. Investing in continuous education strengthens overall risk management. The article argues that modern security strategies must be tightly integrated with training programs. This synergy enhances an organization's ability to withstand crises. The findings underscore training as not only supportive but essential to effective security management.

Key words:
Security management, resilience, risks, employees

1 Ing. David Březina, Technická univerzita ostrava, katedra manažmentu, david.brezina@vsb.cz

1 SECURITY MANAGEMENT AND RESILIENT COMPANIES

In today's dynamic and unstable environment, companies and organizations face increasingly complex security threats. These go beyond physical safety and include cyberattacks, internal risks, and crises caused by natural or social factors, or even a worldwide pandemic. Security management must therefore continuously adapt and implement strategies that not only respond to current threats but also proactively prevent them, so the companies would be in the future much more protected.

A key factor in successfully implementing these strategies is employee education and training. The human factor is often the weakest link in the security chain—but also the one that can make the biggest difference in prevention and response if it is treated professionally. Regular and targeted training increases awareness of potential risks and enables employees to evaluate and respond to incidents effectively.

Well-designed training programs strengthen not only employee knowledge but also a culture of responsibility and vigilance within the organization. Companies that invest in continuous security-related education enhance their resilience to both internal and external challenges, ultimately improving their competitiveness and long-term stability.

While security management shares some similarities with general management, it differs in its focus and objectives. General management is concerned with overseeing an organization's operations and achieving its goals and objectives, while security management is primarily concerned with protecting the organization's assets, employees, and operations from various risks and threats. Security management involves specific techniques and tools, such as risk assessments, threat analysis, incident response planning, and security awareness training. In contrast, general management typically focuses on functions such as planning, organizing, staffing, directing, and controlling. (Ridley, 2023). In summary, security management focus on n identifying and mitigating risks and threats to an organization's security, which differentiates it from general management.

Deficient security may also result from a decision process which sees security as a obligation than a need aligned with one’s business objectives. This naturally leads an organization to aim for a lowest common denominator — for instance, by being standard compliant but not doing anything beyond, or by doing something just about better than a competitor and thus have a false sense of security by falling in the trap of the fallacy of relative deprivation. Such self-delusionary claims of best practices may work as a public relations gimmick, but do not provide robust security, nor facilitate a systematic way to address security concerns. There are various ways to carry out risk analysis. But in all cases, the basic issues to consider include identifying what needs to be protected and the nature of associated threats and vulnerabilities. Accordingly, one needs to determine the consequences of a security breach, typically by assigning a value to the asset in question and accordingly planning the necessary controls to minimize the loss or damage. The desired outcome from a risk analysis is a set

of recommendations to maximize the protection of security objectives while still providing functionality and usability. Such an analysis also needs to take into account the budget constraints — to determine how to allocate limited resources to maximize gains, but also to justify the necessary budget to achieve specific security goals. But the questions needed to be answered are followed: what are the main security risks companies can experience and how are they divided?

The most common types of security are:

1) Physical security
2) Information security
3) Cybersecurity
4) Personnel security
5) Operational security
6) Financial security

Physical security aims s to the measures taken to protect an organization's people, assets, and facilities from physical threats such as theft, vandalism, and terrorism. Physical security measures may include access control systems, surveillance cameras, security guards, and perimeter fencing.
Information security is concerned with protecting an organization's digital assets, including data, software, and hardware, from unauthorized access, use, disclosure, modification, or destruction. Information security measures may include firewalls, antivirus software, encryption, and access controls.
Cybersecurity is a subset of information security that specifically deals with protecting an organization's digital assets from cyber threats, including hackers, viruses, and other malicious software.
Personnel security involves measures to ensure that an organization's employees and contractors are trustworthy and reliable. Personnel security measures may include background checks, security clearances, and ongoing monitoring of employee behaviour.
Operational security is concerned with protecting an organization's operations from disruption or compromise. Operational security measures may include business continuity planning, crisis management, and emergency response planning.
Financial security refers to measures taken to protect an organization's financial assets from fraud, theft, or other forms of financial crimes. Financial security measures may include auditing, fraud detection, and risk management.
In summary, the specific skills, experience, and qualifications required of a security manager will depend on the nature of the organization and its security needs. A security manager may specialize in a specific area of security or require a broad range of knowledge and experience across multiple areas of security (Ridley, 2023).
Once a company is well aware of all possible security risks and set up adequate response to them, would it be possible to call this kind of company already resilient? The answer to this is certainly hard to answer. Resilient do not always mean that companies are well prepared to combat security risks mentioned

above but also must be prepared for external challenges such as unpredictability and unprecedented changes.

The digital revolution has increased the availability of data, the degree of connectivity, and the speed at which decisions are made. This offers transformational promise but also comes with potential for large-scale failure and security breaches, together with rapid cascading of consequences. It also increases the speed at which a company's reputation can change in the eyes of consumers and employees. The changing climate presents structural shifts to companies' risk-return profiles, which will accelerate nonlinearly. Companies need to navigate concerns for their immediate bottom line together with pressures from governments, investors, and society at large. All this while natural disasters are growing more frequent and severe (Nauck, 2021).

Speaking of a reputation and how it can change in the eyes of consumers and employees, current trends show urgent need to be more sustainable and eco-friendlier. Building this resilience means fostering agile, adaptable leaders and teams ready to tackle whatever comes next, from climate events to economic shifts. It's about maintaining strong customer relationships and safeguarding company reputation when challenges arise.

2 INCORPORATING RESILIENCE REQUIREMENTS

Corporate resilience refers to an organization's ability to anticipate, prepare for, respond to, and recover from crises while maintaining long-term sustainability. This includes financial stability, operational adaptability, and the capacity to innovate.

Key Characteristics of Resilient Companies:

1. **Strategic Agility**: Companies that swiftly respond to market changes and consumer demands remain competitive. Agile organizations maintain flexible business models that allow for rapid pivoting in response to external shocks.
2. **Financial Stability**: Maintaining healthy balance sheets, low debt levels, and diversified revenue streams ensures financial resilience during downturns.
3. **Digital Transformation**: Embracing technology enables firms to streamline operations, enhance efficiency, and remain relevant in an evolving marketplace.
4. **Strong Leadership**: Visionary leadership fosters a culture of resilience by promoting adaptability, employee empowerment, and a forward-thinking mindset.
5. **Corporate Culture and Workforce Engagement**: Organizations that prioritize employee well-being, continuous learning, and inclusive decision-making cultivate a workforce that is resilient and innovative. (Agofonova, 2024)

For example, at the personal level strong purpose instils motivation and passion for an employee to learn, to develop, grow and perform. This in turn

cultivates a more engaged workforce and can influence the organization and the sector in which it participates. The same compounding impact moves all the way towards its impact on broader society. Resilience, therefore, is a virtuous cycle. And each level of resilience influence deeply the next form a return on investment perspective as well. Research shows that a purpose-oriented workforce tends to be one that seeks out challenging opportunities, engages in connecting with others to learn faster, and are overwhelmingly confident in its ability to learn and adapt - something that is critical in times of uncertainty (Ruys, 2021).

Security is not solely a technological issue. Human error, negligence, and insider threats are among the leading causes of security breaches. Therefore, cultivating a security-aware organizational culture is critical. This can be achieved through:

- Regular employee training and simulations
- Clear communication of security policies
- Background checks and access restrictions
- Leadership commitment to enforcing compliance

Training employees to adapt is the backbone of a resilient organisation. By building flexibility into company team's skill set, the company empower them to handle change confidently and stay engaged, even in unpredictable situations. Use a mix of training methods—like simulations and role-playing exercises—that mirror real-world challenges.

These hands-on scenarios encourage critical thinking and creative problem-solving, giving teams practical experience in tackling complex situations. Leadership development is a core part of this approach. Adaptive leaders guide their teams through uncertainty, setting an example of resilience and confidence. Invest in programmes that develop these skills, helping leaders inspire self-sufficient, adaptable teams. This not only builds resilience but also fosters a culture where your organisation can thrive, no matter what changes lie ahead. A complicating issue is that preexisting trends in remote work, e-commerce, and automation accelerated during the pandemic, putting some workers in higher demand but displacing many more. In developed and developing nations alike, employers are finding it difficult to hire enough specialized talent to expand. Tech workers, for example, are in high demand in economies large and small, a shortage that may be the best indication of the kind of high-level reskilling organizations need for the economies of the future. Furthermore, IT workers and cybersecurity professionals are now especially sought after, as they are crucial to the rising demands of remote work and building organizational resilience (Pacthod, 2022).

3 RESILIENCE RECOMMENDATIONS

A resilient company is characterised by a strong corporate culture based on trust, openness and transparency. This culture promotes collaboration and exchange between departments and hierarchical levels, which increases joint

problem-solving and innovation. Employees in such an environment feel supported and motivated, which not only increases their satisfaction but also their productivity. Resilient organisations often have a lower turnover rate as they provide a working environment that supports stress management and promotes stress resilience. If employees feel that their employer supports them in difficult times and gives them room for personal and professional development, this significantly increases their loyalty to the company.
The main three recommendations are:

1) **Education and training:** offer regular workshops and training sessions to teach employees how to deal with stress and techniques to improve resilience. In concrete terms, for example, employees can scrutinise their own expectations by deliberately coming up with completely unexpected scenarios. Perception grids can be compared and supplemented in a joint exchange.
2) **Open communication:** Promote a culture of open communication in which employees feel safe to express their concerns and seek support. Regular feedback sessions and additional anonymous channels can help build trust and facilitate dialogue between employees and managers.
3) **Flexibility and autonomy:** Give your employees more autonomy and flexibility to complete their tasks. Flexible working hours and the option to work from home can significantly improve stress management in the workplace.

   (Haushid, 2024)

CONCLUSION

Security management is a dynamic and multidisciplinary field that plays a vital role in protecting organizational assets. As threats evolve, so too must the strategies used to counter them. Resilient companies are those that proactively embrace change, leverage innovation, and cultivate a culture of adaptability. By integrating financial prudence, technological advancements, and strong leadership, organizations can not only survive but also thrive in the face of adversity. Future research should focus on emerging resilience strategies in the context of digitalization and global sustainability efforts.

SOURCES

[1] Ridley, T. 2023. What is security management. Available from: https://www.researchgate.net/publication/369118395_What_is_'security_management'_ChatGPT_and_Tony_Ridley_MSc_CSyP_CAS_MSyl

[2] Fritz, N. 2021. The resilience imperative: Succeeding in uncertain times. Available from: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/the%20resilience%20imperative%20succeeding%20in%20uncertain%20times/the-resilience-imperative-succeeding-in-uncertain-times.pdf

[3] Pacthod, D. 2022. Resilience for sustainable, inclusive growth. Available from: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/resilience%20for%20sustainable%20inclusive%20growth/resilience-for-sustainable-inclusive-growth_final.pdf

[4] Agofonova, I. 2024. On the issue of resilience as a factor for business ecosystems sustainable development. Available from: https://www.researchgate.net/publication/381402610_On_the_issue_of_resilience_as_a_factor_for_business_ecosystems_sustainable_development

[5] Haushild, T. 2024. Resilience in the company: Why it's crucial for both employers and employees. Available from: https://arts.eu/en/insights/article/resilience-in-the-company-why-its-crucial-for-both-employers-and-employees/

ČASOPROSTOROVÁ ANALÝZA KRIMINALITY POMOCÍ METODY NESTACIONÁRNÍHO KLOUZAVÉHO PRŮMĚRU

Karolina Dlouhá[1]

ABSTRAKT

Článek představuje metodu nestacionárního klouzavého průměru (NSMA) pro časoprostorovou analýzu kriminality zaměřenou na efektivnější řízení rizik. NSMA překonává omezení tradičních klouzavých průměrů díky schopnosti reagovat na dynamické a proměnlivé vzorce kriminality. Metoda kombinuje časové vyhlazování a prostorové shlukování pomocí algoritmu K-means pro identifikaci významných kriminálních ohnisek. Navržený přístup je formulován jako vícekriteriální optimalizační problém, kde se vyvažuje prostorové shlukování a časové vyhlazování pomocí regulačního parametru. Aplikace metody na reálná data z České republiky ukazuje její potenciál při odhalování ohnisek kriminality a zlepšování rozhodovacích procesů při prevenci.

Klíčová slova:
Nestacionární klouzavý průměr, časoprostorová analýza, prostorové shlukování, kriminalita.

ABSTRACT

The article presents the Non-Stationary Moving Average (NSMA) method for spatiotemporal crime analysis aimed at more effective risk management. NSMA overcomes the limitations of traditional moving averages by its ability to adapt to dynamic and variable crime patterns. The method combines temporal smoothing and spatial clustering using the K-means algorithm to identify significant crime hotspots. The proposed approach is formulated as a multi-criteria optimization problem, balancing spatial clustering and temporal smoothing through a regularization parameter. The application of the method to real data from the Czech Republic demonstrates its potential for detecting crime hotspots and improving decision-making in prevention efforts.

Key words:
Non-Stationary Moving Average, spatiotemporal analysis, spatial clustering, crime.

1 Ing. Karolina Dlouhá, Fakulta bezpečnostního inženýrství VŠB-TUO, Katedra bezpečnostních služeb, karolina.dlouha@vsb.cz

1 ÚVOD

Zachytit a vyhodnotit proměnlivost kriminality v čase a prostoru je dnes jednou z hlavních výzev při řízení bezpečnostních rizik. S rostoucí dynamikou městského prostředí a proměnlivými vzorci chování se zvyšuje potřeba nástrojů, které umožní včas identifikovat vznikající ohniska trestné činnosti.

Jedním z takových nástrojů je časoprostorová analýza, která propojuje informace o čase a místě výskytu událostí. Tento článek představuje metodu Nestacionárního klouzavého průměru (NSMA), jež umožňuje sledovat kriminalitu z obou hledisek současně.

NSMA navazuje na klasické analytické přístupy, ale rozšiřuje je o schopnost přizpůsobit se proměnlivým podmínkám. Spojuje časové vyhlazování s prostorovým shlukováním a využívá optimalizační model, který obě složky propojuje do jednoho celku.

2 VSTUPNÍ DATA A JEJICH CHARAKTERISTIKA

Analýza byla provedena na základě reálných dat o kriminalitě v České republice za kalendářní rok 2024, která byla poskytnuta Policií České republiky. Jedná se o strukturovaný soubor incidentů, v němž každý záznam představuje jednu zaznamenanou událost spadající do kategorie obecné kriminality.

Každý záznam v datovém souboru obsahuje následující atributy:
- čas nahlášení události (datum a čas),
- geografickou polohu ve formě zeměpisných souřadnic,
- typ trestné činnosti a
- stav vyšetřování [6].

Pro účely modelování byla každá událost popsána jako dvojice $[\tau_i, X_i]$, kde $\tau_i \in \mathbb{R}$, představuje čas události a $X_i \in \mathbb{R}^2$ její polohu.

Z těchto dat byla sestavena časová řada denních počtů incidentů, značená $\varphi(t)$, která následně sloužila jako podklad pro vyhlazování pomocí klouzavého průměru. Z prostorových údajů bylo vytvořeno pole pro prostorové shlukování metodou K-means.

Před zpracováním byla provedena filtrace neúplných nebo chybně zaznamenaných dat, aby byl zajištěn jednotný formát pro vstup do analytických metod. Výsledný datový soubor obsahoval tisíce incidentů, pokrývajících území celé České republiky.

3 METODOLOGIE

3.1 PROSTOROVÉ SHLUKOVÁNÍ – METODA K-MEANS

Pro identifikaci prostorových vzorců kriminality byla použita metoda K-means, která rozděluje události do K shluků na základě jejich geografické polohy. Každý shluk je reprezentován svým středem (tzv. centroidem) a algoritmus minimalizuje součet čtvercových vzdáleností mezi událostmi a jejich příslušnými centroidy [1,4].

Formálně hledáme optimální rozdělení:

$$[C^*,\ \Gamma^*] := \arg\min_{\Gamma\in\Omega_\Gamma} \underbrace{\sum_{i=1}^{N}\sum_{k=1}^{K}\Gamma_{k,i}\cdot\left\|X_{:,i}-C_{:,k}\right\|_2^2}_{=:f\ (C,\Gamma)}, \tag{1}$$

kde X_i značí polohu události, $C_k$pozici centroidu a $\Gamma_{k,i}$ příslušnost k danému shluku. Řešení probíhá iterativně střídavou aktualizací přiřazení a výpočtu středů. Výsledkem je prostorové rozdělení kriminality na kompaktní oblasti s podobnou mírou výskytu [5].

3.2 NESTACIONÁRNÍ KLOUZAVÝ PRŮMĚR

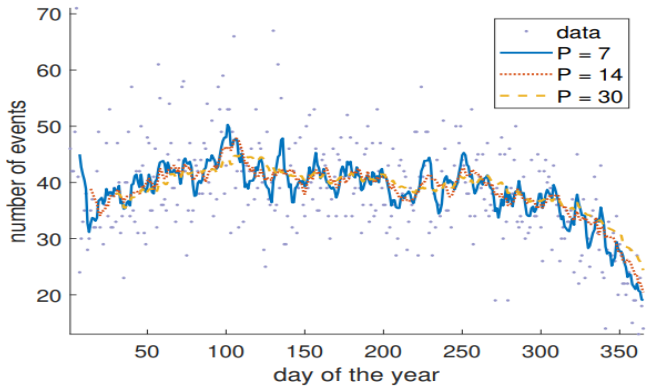
Pro analýzu časového průběhu kriminality byla použita metoda nestacionárního klouzavého průměru (NSMA), která rozšiřuje běžně používaný klouzavý průměr (MA) o schopnost rozlišit více typů chování v čase. Zatímco klasický klouzavý průměr aplikuje jednotné vyhlazení na celou časovou řadu, NSMA umožňuje adaptivně přizpůsobit vyhlazení různým skupinám událostí, které vykazují podobné časové charakteristiky [1,2].

Základní časová řada událostí je označena jako $\varphi(t)$, kde každý prvek představuje počet trestných činů zaznamenaných v daném dni t. Tato řada přirozeně kolísá v čase (například sezónně nebo podle dne v týdnu), což motivuje použití vyhlazovacích metod [1,3].

Klasický klouzavý průměr vypočítává průměr z předchozích P dnů:

$$\hat{\varphi}(t) := \frac{1}{P}\sum_{p=1}^{P}\varphi(t-p). \tag{2}$$

Účinek různé volby parametru P na vyhlazení časové řady je dobře patrný na obrázku 1, který ukazuje denní počty kriminálních událostí v roce 2024 vyhlazené klouzavým průměrem s různou délkou okna (7, 14 a 30 dní). Je zřejmé, že čím větší je hodnota P, tím hladší je výsledná křivka, ale zároveň dochází ke ztrátě detailu [2].



Obrázek 1 Vliv velikosti vyhlazovacího okna PPP na tvar časového průběhu klouzavého průměru [2].

Metoda NSMA tuto myšlenku rozšiřuje tak, že incidenty jsou rozděleny do několika skupin podle podobnosti jejich výskytu v čase. Každé skupině k je přiřazena samostatná časová řada $\varphi_k(t)$ a její vlastní vyhlazený průběh:

$$\varphi_k(t) := \sum_{i \in \mathcal{N}} \gamma_k(i),\ \hat{\varphi}_k(t) := \frac{1}{P} \sum_{p=1}^{P} \varphi_k(t-p). \tag{3}$$

Celkový odhadovaný průběh pak vzniká jako součet všech vyhlazených časových řad:

$$\hat{\varphi}(t) = \sum_{k=1}^{K} \widehat{\varphi_k}(t) \tag{4}$$

Úkolem metody je nalézt takové rozdělení incidentů do skupin (zachycené pomocí maticové proměnné Γ), které minimalizuje rozdíl mezi původním a vyhlazeným časovým průběhem:

$$\Gamma^* = \arg\min_{\Gamma \in \Omega_\Gamma} \sum_t (\varphi(t) - \hat{\varphi}(t))^2 \qquad (5)[2]$$

Protože původní binární přiřazení (každá událost náleží právě jedné skupině) je výpočetně náročné, zavádí se relaxace: přiřazení je nahrazeno spojitými hodnotami v rozmezí od 0 do 1. Tím vzniká tzv. rozšířená množina:

$$\widehat{\Omega_\Gamma} := \left\{ \Gamma \in [0,1]^{K,N} \,|\forall_i : \sum_{k=1}^{K} \Gamma_{k,i} = 1 \right\} \qquad (6)[2]$$

Díky tomuto způsobu přiřazení je možné úlohu řešit výpočetně jednodušeji a rychleji pomocí běžně dostupných optimalizačních metod.

3.3 VÍCEKRITERIÁLNÍ OPTIMALIZACE

Zatímco předchozí části se zabývaly odděleně prostorovým shlukováním a časovým vyhlazováním, cílem této části je propojit obě složky do jednoho společného modelu. Navržený přístup umožňuje současně zohlednit, kde se trestné činy vyskytují, a zároveň kdy a s jakou intenzitou [1].

Tato úloha je formulována jako vícekriteriální optimalizace, kde se hledá takové přiřazení událostí ke skupinám a odpovídající prostorová centra, které co nejlépe vyhovují dvěma cílům:

- minimalizovat prostorovou rozptýlenost jednotlivých skupin (viz část 3.1),
- dosáhnout co nejpřesnějšího časového vyhlazení pomocí NSMA (viz část 3.2) [2].

Kombinovaná optimalizační úloha je vyjádřena takto:

$$[C^*, \Gamma^*] := \arg\min_{\Gamma \in \Omega_\Gamma} \frac{1}{N} f(C, \Gamma) + \frac{\varepsilon}{T} g(\Gamma), \tag{7}$$

kde:

- $f(C, \Gamma)$odpovídá prostorové části modelu (viz rovnice (1)),
- $g(\Gamma)$ představuje chybu časového vyhlazení, které můžeme definovat jako:

$$\Gamma^* = \arg\min_{\Gamma \in \Omega_\Gamma} \underbrace{\sum_t (\varphi(t) - \hat{\varphi}(t))^2}_{=:\, g(\Gamma)}, \tag{8}$$

- $\varepsilon \geq 0$ je parametr, který určuje, jak velkou váhu má časové hledisko vůči prostorovému.[2]

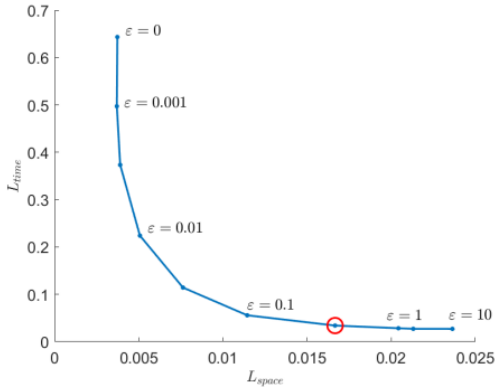
Pomocí tohoto parametru lze ovlivnit, zda bude výsledek více respektovat podobnost v prostoru, nebo v čase. Jeho vhodná volba je klíčová pro dosažení vyváženého řešení.

Samotné řešení této úlohy vychází z principu střídavé optimalizace – nejprve se aktualizují prostorové pozice středů shluků C, poté se přepočítá přiřazení událostí Γ, a tento proces se opakuje, dokud nedojde ke stabilizaci výsledku. Stejně jako v předchozích částech se zde využívá spojité přiřazení, které usnadňuje výpočet [1].

4 VÝSLEDKY

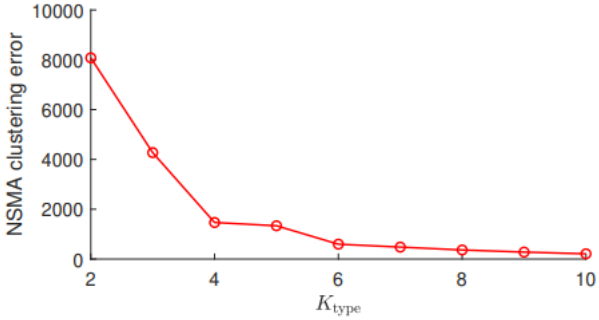
Navržená metodika byla implementována v prostředí MATLAB a aplikována na soubor reálných dat o obecné kriminalitě zaznamenané v České republice v roce 2024. Pro časové vyhlazování byl zvolen klouzavý průměr s délkou okna $P = 7$, což odpovídá týdennímu průměru.

Počet prostorových shluků byl nastaven na $K = 30$. Výběr vhodné hodnoty agregačního parametru ε, který vyvažuje časové a prostorové hledisko v optimalizační úloze (viz rovnice (10)), byl proveden na základě tzv. L-křivky. Ta znázorňuje kompromis mezi chybou prostorového shlukování a chybou časového vyhlazení. Optimální hodnota byla stanovena jako $\varepsilon = 10^{0,5}$, což představuje rovnovážný bod mezi oběma složkami modelu (viz obrázek 2) [2].



Obrázek 2 Výběr optimální hodnoty parametru ε\varepsilonε pomocí L-křivky [2].

Při počátečním nastavení vzniklo několik prostorových shluků, které byly téměř nebo zcela prázdné. Tyto skupiny byly odstraněny, a následně bylo provedeno další shlukování na základě podobnosti časových průběhů NSMA v jednotlivých shlucích. Tím došlo k výraznému zjednodušení struktury: prostorové shluky byly sloučeny do šesti hlavních typů kriminality podle podobnosti jejich časového vývoje (viz obrázek 3) [2].



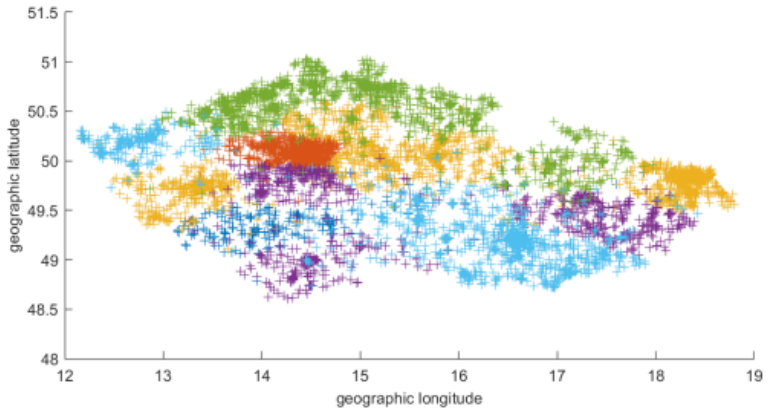
Obrázek 2 Identifikace optimálního počtu typů časových průběhů pomocí elbow method [2].

Výsledná typologie zahrnuje:

- skupiny s vyrovnaným výskytem v průběhu roku,
- typy s nárůstem v letních měsících,
- typy s výraznými výkyvy či sezónním charakterem [2].

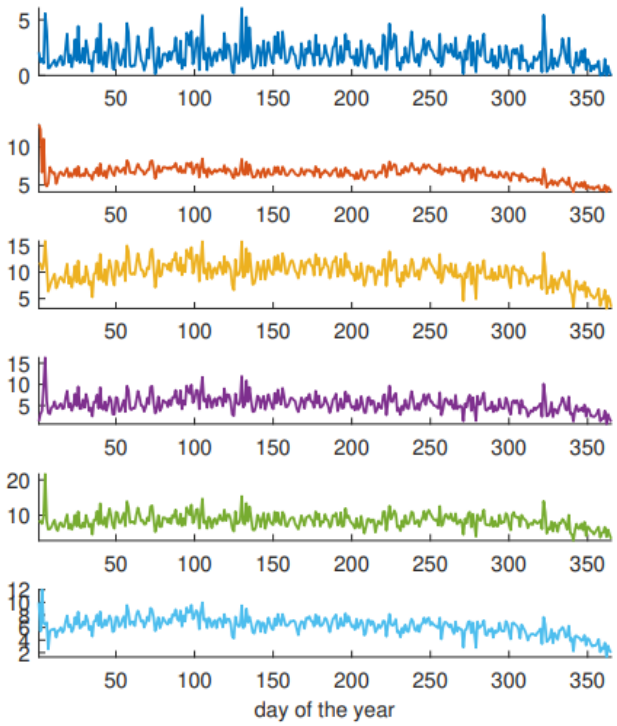
Tato kategorizace umožňuje lépe porozumět dynamice vývoje kriminality v různých částech České republiky.

Obrázek 4 zobrazuje výsledné prostorové rozložení jednotlivých typů, přičemž každý bod (incident) je barevně označen podle typu, do kterého byl zařazen. Výsledné typy mají zřetelně odlišené geografické rozložení a zároveň reprezentují odlišné časové chování.



Obrázek 3 Výsledné prostorové rozložení typů kriminality na území České republiky [2].

Obrázek 5 pak ukazuje odpovídající časové průběhy klouzavých průměrů pro jednotlivé typy. Tyto křivky poskytují přehled o tom, jak se jednotlivé formy kriminality vyvíjely v průběhu roku – například zda měly stabilní průběh, sezónní vrcholy nebo krátkodobé nárůsty.



Obrázek 4 Časové průběhy kriminality pro jednotlivé typy určené metodou NSMA [2].

5 DISKUSE A PŘÍNOS

Výsledky ukazují, že navržená metoda dokáže zachytit významné časoprostorové vzorce kriminality. Spojením prostorového shlukování a nestacionárního časového vyhlazování lze identifikovat nejen místa s vyšší kriminalitou, ale i odlišnosti v jejich časovém vývoji.

Metoda umožňuje vyhladit náhodné výkyvy, odhalit dlouhodobější trendy a přizpůsobit důraz na prostorovou či časovou složku podle potřeby. Výstupy jsou srozumitelné a prakticky využitelné – například při plánování policejních opatření nebo hodnocení účinnosti prevence.

6 ZÁVĚR

V tomto článku byla představena metoda, která umožňuje současně sledovat prostorové i časové souvislosti kriminality. Kombinací klasického klouzavého průměru s metodou K-means vznikl nástroj, který dokáže přehledně zobrazit vývoj kriminality v čase a zároveň zachytit její geografické rozložení.

Aplikace na reálná data z České republiky ukázala, že metoda dobře odhaluje oblasti s vyšším výskytem událostí i jejich rozdílnou dynamiku během roku. Výsledky mohou napomoci lepšímu plánování prevence i cílenému rozmisťování bezpečnostních sil.

V budoucnu lze uvažovat o využití tohoto přístupu také pro jiné typy incidentů nebo o jeho rozšíření o predikční schopnosti.

LITERATURA

[1] DLOUHÁ, K. (2024). Kauzalitní modelování v oblasti bezpečnosti. Diplomová práce. Ostrava: VŠB – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství.

[2] DLOUHÁ, K., POSPÍŠIL, J., ŠČUREK, R. (2025). Spatiotemporal Crime Analysis for Risk Management Using the Non-Stationary Moving Average Method. In: Proceedings of the European Safety and Reliability Conference (ESREL 2025). Southampton, UK: Research Publishing, in print.

[3] DLOUHÁ, K., POSPÍŠIL, J. (2024). Non-Stationary Moving Average Method for Time Series Decomposition in Risk Analysis. In: Proceedings of the International Conference on Numerical Analysis and Applied Mathematics (ICNAAM 2024). Heraklion, Greece: American Institute of Physics, in print.

[4] HORENKO, I. (2010). Finite element approach to clustering of multidimensional time series. SIAM Journal on Scientific Computing, 32(1), pp. 62–83.

[5] PFEIFER, P., DEUTSCH, S. J. (1980). A three-stage iterative procedure for space-time modeling. Technometrics, 22(1), pp. 35–47.

[6] The Police of the Czech Republic (2024). Crime statistics. Online. Available from: https://kriminalita.policie.cz [ref. 2025-01-07]

VLIV RASTROVÉHO PODHLEDU NA FUNKCI SPRINKLEROVÝCH HLAVIC

Michal Dvořák[1]

ABSTRAKT

S rozvojem požární ochrany byly do praxe zavedeny stabilní hasicí zařízení, která mají významný vliv na omezení šíření požáru nebo jeho úplné uhašení. Samočinné stabilní hasicí zařízení reaguje na požár již ve fázi jeho vzniku, což umožňuje rychlou intervenci. Avšak přítomnost podhledů může představovat omezení pro správnou funkci těchto hasicích zařízení. Typickým příkladem je instalace hasicího systému v obchodním centru, následovaná instalací podhledu, který má zejména estetický designový účel. Tato konfigurace může negativně ovlivnit schopnost stabilního hasicího zařízení. Příspěvek poukazuje na problematiku interakce sprinklerových hlavic nad instalovaným rastrovým podhledem.

Klíčová slova:
Sprinklerové hlavice, rastrový podhled, interakce

ABSTRACT

With the development of fire protection, stable fire extinguishing devices have been introduced into practice, which have a significant impact on limiting the spread of fire or extinguishing it completely. A self-propelled fixed fire extinguishing system reacts to a fire at its outset, allowing rapid intervention. However, the presence of false ceilings may pose a limitation to the proper functioning of these extinguishing devices. A typical example is the installation of a fire extinguishing system in a shopping centre, followed by the installation of a suspended ceiling, which has a mainly aesthetic design purpose. This configuration can adversely affect the ability of a stable fire suppression system. This paper highlights the issue of sprinkler head interaction over an installed raster ceiling.

Key words:
Sprinkler heads, raster (open) ceiling, interaction

1 Ing. Michal Dvořák, Fakulta bezpečnostního inženýrství VŠB-TUO, michal.dvorak@vsb.cz

1 ÚVOD

Požární ochrana je klíčovým aspektem bezpečnosti staveb, který musí být zohledněn při plánování výstavby, například obchodních center. Kromě parametrů, jako jsou únikové cesty či statická stabilita, je nutné zajistit ochranu nosných konstrukcí a použití požárně bezpečnostních zařízení, jako je například stabilní hasicí zařízení (dále jako SHZ). SHZ slouží k rychlému potlačení požáru a minimalizaci škod na majetku i životech. Jejich návrh vychází z požadavků norem, odborných dokumentů a dalších specifik.

Klíčovým faktorem je nejen volba hasicího média a hlavic, ale také jejich umístění, které ovlivňuje účinnost systému. Technologické rozvody mohou být instalovány do podhledové konstrukce či nad ní, což přináší otázky ohledně distribuce vody při hašení. Aby bylo zajištěno efektivní fungování, je třeba vzít v úvahu vliv podhledu na rozptyl vody a přizpůsobit návrh konkrétním podmínkám budovy.

To, jak se voda dostane k ohnisku požáru záleží na mnoha faktorech. Volba hlavice, vzdálenost hlavic od podhledu, vzhled rastru a jeho velikost, použitý tlak na hlavici, vliv ventilace v objektu a tím omezení dopadu vody na správné místo.

Tento příspěvek nastíní alespoň základní poznatky potřebné k určení vlivu rastrové konstrukce na distribuci vody ze sprinklerové hlavice.

2 SPRINKLEROÉ HLAVICE

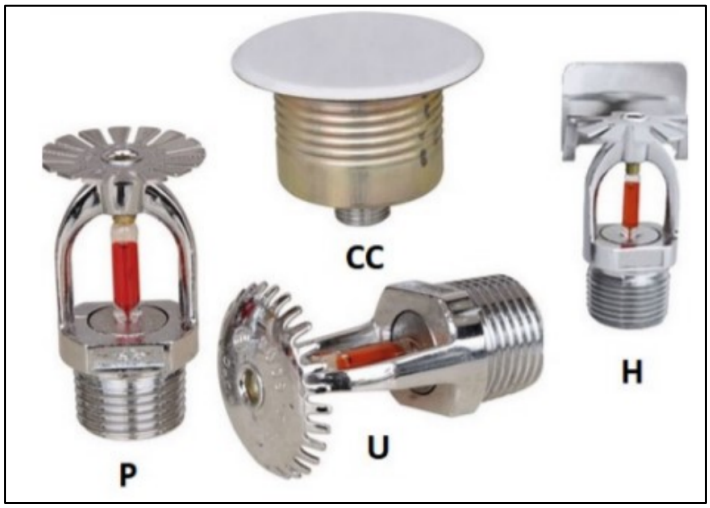
Jedná se o samočinné zařízení, které se v případě požáru za splnění určitých podmínek aktivuje a lokalizuje, či likviduje požár. K otevření sprinklerové hlavice je třeba zahřát pojistku na otevírací teplotu. Při zahřátí dojde k roztavení nebo roztržení pojistky z důvodu zvětšení objemu kapaliny, která se v pojistce nachází [1].

Pro správnou funkci je důležité vždy vybrat správnou hlavici. Existuje poměrně velké množství výrobců, ale především různých variant provedení. U hlavic nás zajímá především následující vlastnosti [1-2]:

- **Otevírací teplota** – lze rozeznávat podle barev (například červená 68 °C)
- **Tepelná odezva** – tepelná odezva sprinklerové hlavice, měřená indexem reakční doby (RTI), určuje rychlost dosažení otevíracích teplot. Citlivost lze upravit změnou objemu skleněné baňky nebo úpravou plochy a tloušťky tavných pojistek.
- **Výstřikový parametr** – konstrukce tříštiče sprinklerové hlavice určuje rozvržení vody a ovlivňuje distribuci vody, tvar a délku výstřikového proudu.
- **Umístění** – umístěné hlavice může být stojaté (U), závěsné (P), horizontální (H), zapuštěné/polozapuštěné (L, R) nebo zakryté (CC), což

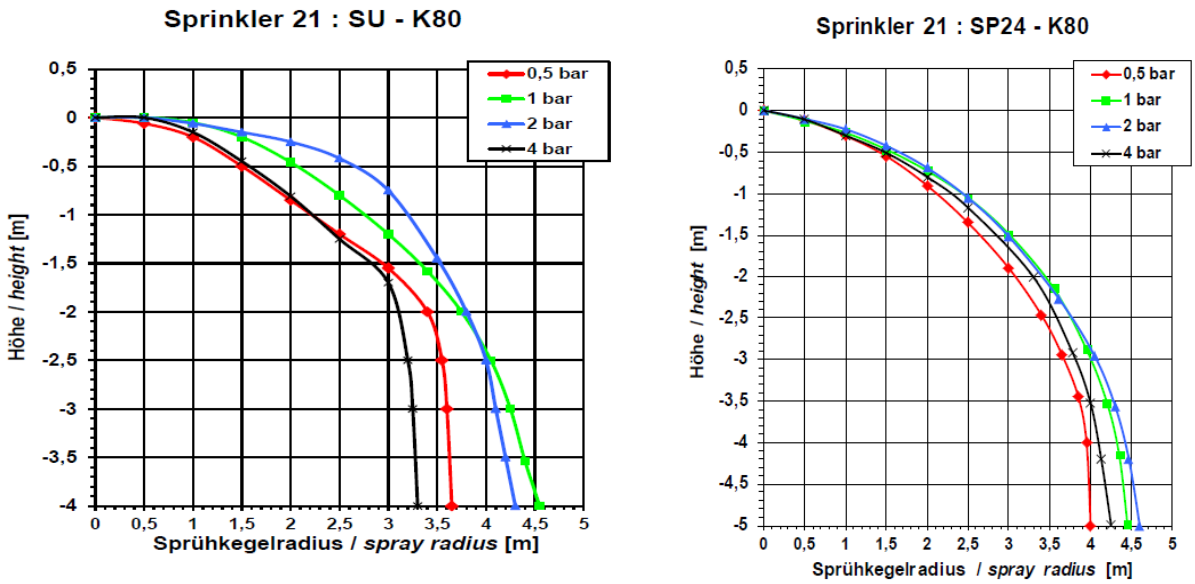
ovlivňuje jejich hasicí schopnosti, respektive rozptyl vody. Různé varianty hlavic můžeme vidět na obrázku 1 (Obrázek 1).

- **K faktor** – množství vody, které je sprinklerová hlavice schopna dodat k požáru.



Obrázek 1 Různé varianty sprinklerových hlavic [3]

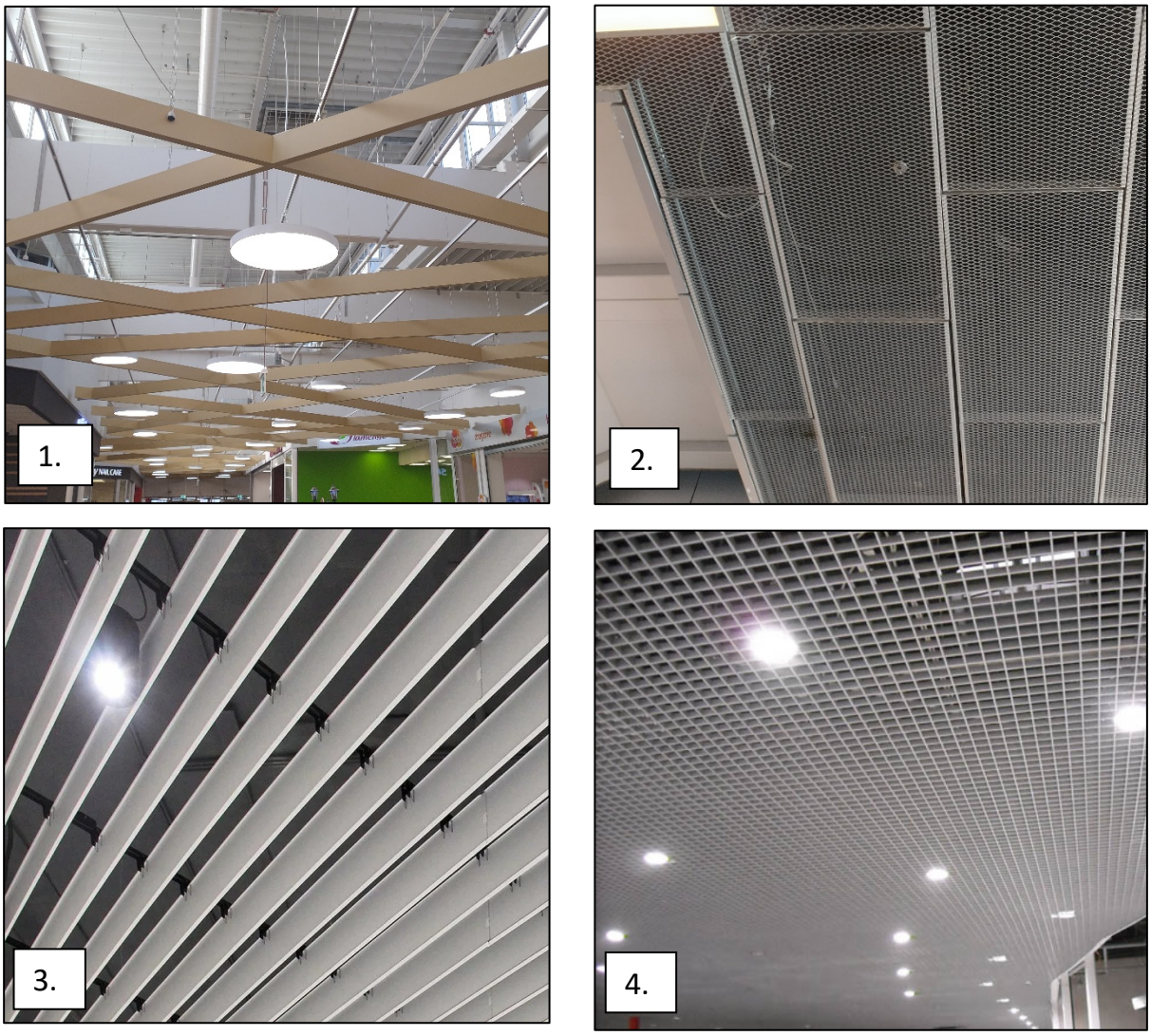
Již samotná volba, zda zvolíme hlavici stojatou, nebo ležatou nám napovídá, která z nich bude vhodnější pro distribuci vody vzhledem k podhledu. Na obrázku 2 (Obrázek 2) můžeme vidět rádius, tedy dostřik (rozptyl) vody pro stojatou hlavici SU a dále pak pro ležatou SP. Například pokud vzdálenost hlavice od podhledu bude cca 80 cm tak pro SU bude rádius 3 m a pro SP 2 m. Tyto charakteristiky se však vždy liší a je třeba stanovit nejvíc optimální hlavici vzhledem k druhu a vzdálenosti rastru. Další kapitola popisuje různé varianty podhledů pod těmito sprinklerovými hlavicemi.



Obrázek 2 Rádius rozstřiku vody SU – stojatá hlavice, SP – ležatá hlavice [4-5]

2 RASTROVÁ PODHLEDOVÁ KONSTRUKCE

Rastrová podhledová konstrukce je typ zavěšeného stropu, který je tvořen pravidelnou mřížkovou strukturou (rastrem). Rastrové podhledy se často používají v kancelářích, průmyslových objektech nebo veřejných budovách díky jejich flexibilitě a možnosti snadné úpravy. Jedná se zejména o vizuální prvek stropní konstrukce, nad kterou se nachází různé technologie. Různé varianty podhledů můžeme vidět na následujícím obrázku (Obrázek 3).



Obrázek 3 Různé varianty podhledové konstrukce (vlastní fotky)

Rastrové podhledy mohou být vyrobeny z různých materiálů, například kovu, sádrokartonu nebo minerálních desek, a jejich design může být přizpůsoben estetickým i funkčním požadavkům. Za jakých podmínek však můžeme takovýto rastr instalovat pod sprinklerovými hlavice nastiňuje následující kapitola popisují podmínky jednotlivých norem a předpisů.

3 POŽADAVKY NA PODHLEDOVÉ KONSTRUKCE V SOUVISLOSTI S INSTALACÍ SPRINKLEROVÝCH HLAVIC

Pro navrhování sprinklerových hlavic nad rastrovým podhledem na území ČR známe několik norem a předpisů. V České republice je zásadní harmonizovaná evropská norma **ČSN EN 12 845 + A1** z května 2020, která stanovuje požadavky a doporučení pro návrh, montáž a údržbu. Ve Spojených státech amerických platí norma **NFPA 13 – Standart for the Installation of Sprinklers Systemsb**, která se rovněž zaměřuje na návrh a instalaci těchto systémů. Mezi mezinárodní dokumenty patří například **FM Global Property Loss Prevention Data Sheets 2-0**, poskytující pokyny pro instalaci automatických sprinklerů. Tyto normy se věnují mimo jiné návrhům hlavic umístěných nad podhledy a stanovují podmínky, za jakých je možné takové řešení použít. Následující část nastiňuje stěžejní podmínky instalace podhledu pod sprinklerovými hlavicemi [6-8].

3.1 ČSN EN 12 845 + A1

V rámci normy je rastrový podhled popsaný jako **„suspended open cell ceilling“**, tedy zavěšený podhled s otevřenými okny (buňkami). Tyto podhledy lze použít ve třídě nebezpečí LH a OH za splnění následujících podmínek.

- Celková půdorysná otevřená plocha stropu, včetně svítidel není menší než **70 %** půdorysné plochy stropní konstrukce
- Minimální rozměr otvorů není menší než **2,5 cm**, nebo není menší než tloušťka závěsného podhledu, podle toho, jaká z hodnota je větší.
- Konstrukční integrita podhledové konstrukce nebo jiného vybavení (svítidla např.) nebudou ovlivňovat provoz sprinklerového zařízení
- Pod stropem nejsou žádné úložné (skladovací) prostory

Kromě výše popsaného je třeba brát v úvahu výšku hlavice nad podhledem. Vzdálenost sprinklerové hlavice od podhledu nesmí přesáhnout vzdálenost **300 cm.** Rovněž svislá vzdálenost mezi sprinklerem a horní částí zavěšeného podhledu nesmí být menší, než **80 cm.** Poslední poznámkou k provedení je, že v případě vyskytujících se překážek s šířkou větší než 80 cm musí být doplněny doplňkové sprinklery ke zkrápění pod překážkami (např. zmiňované světlo).

3.2 NFPA 13

Americká norma NFPA 13 stanovuje pravidla pro návrh a instalaci sprinklerových systémů, minimalizujících riziko požáru, ztráty majetku a životů. U stropů s otevřenou mřížkou musí mít otvory šířku nejméně **0,6 cm**, jejich výška nesmí přesáhnout šířku, a podhled musí být alespoň z **70 %** otevřený.

Minimální vzdálenost mezi podhledem a sprinklerovou hlavicí je **45 cm** pro lehké nebezpečí s roztečí hlavic do 3 m × 3 m. Při větší rozteči hlavic narůstá vzdálenost na 60 cm, 90 cm a až 120 cm vzhledem k rozptylu vody ze sprinkleru.

3.3 FM GLOBAL INSTALLATION GUIDELINES FOR AUTOMATIC SPRINKLERS

Jedná se o americkou pojišťovací společnost zaměřující se na prevenci škod, jejíž klienty jsou především velké korporace s vysokým rizikem v oblasti pojištění majetku. Tento guideline poskytuje doporučení pro instalaci sprinklerových systémů, které rozděluje na systémy pro skladovací a neskladovací prostory. Zahrnuje také stropy typu **Open-Grid Ceiling**, tedy podhledy (stropy) s otvory tvořícími nejméně **70 %** plochy.

Guideline avšak detaile neřeší podmínky instalace sprinklerů nad rastrovým podhledem. Najdeme zde zejména podmínky instalace sprinklerů **pod** podhledem nikoliv nad ním. Kromě podmínky otevřenosti 70 % stropní plochy zde další podmínky nenalezneme.

3.4 VDS CEA 4001 SPRINKLER SYSTEMS, PLANNING AND INSTALLATION [9]

Jedná se o německé pokyny upravují instalaci a údržbu pevných sprinklerových systémů v budovách a průmyslových objektech, včetně požadavků na ochranu života, klasifikace rizik, vodních zdrojů, instalace a testování. Použití podhledů pod sprinklery je omezeno na třídy rizika LH, OH za těchto podmínek:

- Celková otevřená plocha zavěšeného otevřeného podhledu, včetně svítidel, musí být větší než **70 %** plochy plánovaného stropu
- Minimální rozměr stropních otvorů nesmí být menší než **2,5 cm** nebo menší než vertikální tloušťka zavěšených stropů, podle toho, která z hodnota je větší
- Strukturální celistvost stropu a veškerého dalšího vybavení, jako jsou například svítidla, nesmí ovlivňovat provoz sprinklerového systému

4 ŘEŠENÉ PRÁCE NA DANOU PROBLEMATIKU

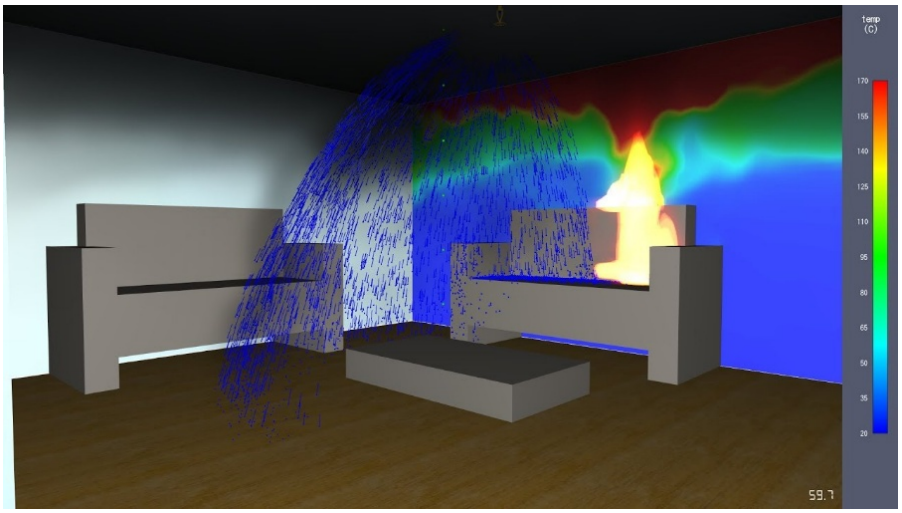
Mezi současně řešené a stěžejní práce můžeme zařadit následující 2 práce. Diplomová práce „**Vliv podhledové konstrukce na funkci systému stabilního hasicího zařízení**“ zkoumá vliv perforovaného podhledu na účinnost sprinklerových hlavic. Experimenty sledovaly distribuci vody při různých výškách podhledu a tlacích vody. Teoretická část popisuje princip hašení, technické normy a vlastnosti sprinklerů, zatímco experimentální část ukazuje, jak se mění rozptyl vody v závislosti na podhledu. Nejmenší odchylky byly zaznamenány při

umístění podhledu 0,3 m pod sprinklerovou hlavicí, zatímco větší odchylky nastaly při výškách 0,65 m a 1 m, kde konstrukce měnila trajektorii kapek a snižovala efektivitu pokrytí. Experiment upozorňuje na riziko nerovnoměrného rozptylu vody u některých podhledových konfigurací a doporučuje zmenšit rozestupy mezi hlavicemi při instalaci podhledu, zejména při větších vzdálenostech od sprinkleru. Při experimentu byl pouze použit jeden druh rastru, a to ještě po domácku vyrobený, což dále může zkreslovat výsledky práce. Voda ze sprinklerové hlavice byla na zemi měřena sítí kelímků, které se následně vážili [10].

Mezi zahraničními pracemi je důležité zmínit práci „**Study of Grid Ceiling on Parametric Optimization Design of Automatic Sprinkler Systém**“. Práce zkoumá optimalizaci sprinklerového systému s mřížkovým stropem. Distribuce vody je ovlivněna mírou průhlednosti stropu a výškou instalace sprinkleru. Experimenty této práce ukázaly, že s poklesem těchto parametrů se zvyšuje distribuce vody. Měření však opět probíhalo na jednom rastru vlastní výroby. Voda byla měřena formou sítě kelímků na zemi [11].

5 DALŠÍ ZKOUMÁNÍ VZÁJEMNÉ INTERAKCE

Jak je vidět, vzájemné ovlivňování sprinklerové hlavice, tedy roztříštěné vody z něj já dáno mnoha faktory. Vzdálenost, druh rastru, druh hlavice, tlak vody apod. Pro detailnější prozkoumání je potřeba provést další měření, a to zejména na konkrétních druzích podhledů a z těchto měření následně vyvodit závěry. Kromě fyzického experimentu s různými druhy hlavic a podhledy se v dnešní době nabízí možnost modelování v programech je Fire Dynamic Simulation jak je vidět na obrázku 4 (Obrázek 4). Tyto modely umožnují zkoumání rozptylu vody. Výhodou těchto pokusů může být možnost četného opakování nebo i jednoduchost co se týče provedení. Na druhou stranu je třeba mezi modelem a reálným experimentem provést validaci získávaných dat.



Obrázek 4 Rozptyl vody z hlavice v FDS [12]

LITERATURA

[1] RYBÁŘ, Pavel. Sprinklerová zařízení. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2011. ISBN 978-80-7385-106-4.

[2] BEBČÁK, Petr. Požárně bezpečnostní zařízení. 2. rozšířené vydání. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2004. ISBN 80-86634- 34-5.

[3] MAIXNEROVÁ, Eliška. Experimentální stanovení plošné intenzity zkrápění sprinklerovou hlavicí. Ostrava, 2019. Diplomová práce. VŠB-TUO. Vedoucí práce Ing. Dana Chudová, Ph.D.

[4] Hlavice MX5 - SU. Online. Dostupné z: https://www.viking-emea.com/product/mx1001/. [cit. 2025-04-04].

[5] Hlavice MX5 - SP. Online. Dostupné z: https://www.viking-emea.com/product/mx5-sp/. [cit. 2025-04-04].

[6] Stabilní hasicí zařízení - Sprinklerová zařízení - Navrhování, instalace a údržba: ČSN EN 12845. Srpen 2018. Český normalizační úřad, Praha: ÚNMZ, 2018.

[7] NFPA 13: Standard for the Installation of Sprinkler Systems. Quincy, Massachusetts: National Fire Protection Association, 2024 [cit. 2025-04-04].

[8] INSTALLATION GUIDELINES FOR AUTOMATIC SPRINKLERS. Online. FM Global Property Loss Prevention Data Sheets 2-0. 2018. Dostupné z: https://fireprotectionsupport.nl/wp-content/uploads/2019/05/FMDS0200-jan-2018.pdf. [cit. 2025-04-04].

[9] CEA 4001: CEA 4001 Sprinkler Systems: Planning and Installation. Brusel, 2009 [cit. 2025-04-04].

[10] BACA, Jakub. Vliv podhledové konstrukce na funkci systému stabilního hasicího zařízení. Online, Diplomová práce. Ostrava: Vysoká škola báňská - Technická univerzita Ostrava, 2020. Dostupné z: http://hdl.handle.net/10084/140314. [cit. 2025-04-04].

[11] XIANG-YU QUA, Hai-yan Wub. Study of Grid Ceiling on Parametric Optimization Design of Automatic Sprinkler System. ScienceDirect. Fire Protection Bureau of Tongling City, China, , 6. [cit. 2025-04-04].

[12] Převzato z:. Online. Dostupné z: https://www.youtube.com/watch?v=wVvdVw5W1fo&ab_channel=ThunderheadEngineering. [cit. 2025-04-04].

VLIV ŠÍŘKY DUTINY A POVRCHOVÉ ÚPRAVY DŘEVĚNÉ FASÁDY NA VÝŠKU PLAMENE

Stanisław Franek[1], Jakub Klezla[2], Michal Dvořák[3]

ABSTRAKT

V tomto článku je popsáno experimentální měření, které se zaměřuje na analýzu změny výšky plamene v dutině provětrávané fasády z dřevěných palubek, přičemž klade důraz na vliv šířky dutiny a úpravy vnitřního povrchu. V rámci studie bylo provedeno 13 požárních zkoušek s různými variantami dutin a povrchových úprav. Data získaná z měření teplot, tepelného výkonu a kamerových záznamů poskytují důležité poznatky pro optimalizaci požární bezpečnosti dřevěných fasádních systémů.

Kľúčové slová:
provětrávaná fasáda, výška plamene, teplota, tepelný výkon

ABSTRACT

This paper presents an experimental measurement that focuses on to analyze the change in flame height in the cavity of a ventilated wooden façade, emphasizing the effect of cavity width and finishing of the internal surface. As part of the study, 13 fire tests with different variations of cavities and surface treatments. Data obtained from temperature measurements, thermal performance and video recordings provide important insights for optimizing fire safety of wooden façade systems.

Key words:
ventilated facade, flame height, temperature, heat output

1 Stanisław Franek, Ing., VŠB – TUO, Fakulta bezpečnostního inženýrství, Lumírova 13, 700 30 Ostrava - Výškovice, stanislaw.franek@vsb.cz
2 Jakub Klezla, Ing., VŠB – TUO, Fakulta bezpečnostního inženýrství, Lumírova 13, 700 30 Ostrava - Výškovice, jakub.klezla@vsb.cz
3 Michal Dvořák, Ing., VŠB – TUO, Fakulta bezpečnostního inženýrství, Lumírova 13, 700 30 Ostrava - Výškovice, michal.dvorak@vsb.cz

1 ÚVOD

Se vzrůstajícím důrazem na udržitelnost se dřevo stává klíčovým materiálem v moderním stavebnictví. Jeho ekologické vlastnosti, schopnost snižovat uhlíkovou stopu a výborné tepelně izolační vlastnosti z něj činí atraktivní volbu pro výstavbu. Díky moderním technologiím lze dřevo efektivně využít nejen při stavbě rodinných domů, ale i vícepodlažních objektů a složitých architektonických prvků [1,2].

Provětrávané fasádní systémy nabízejí kombinaci ochrany proti klimatickým vlivům, energetické efektivity a estetické hodnoty. Využití dřeva jako vnějšího obkladu v těchto systémech však přináší nové výzvy v oblasti požární bezpečnosti, zejména kvůli možnosti šíření plamene v provětrávané dutině a vzniku komínového efektu [1-3].

Požární bezpečnost provětrávaných fasádních systémů se tak stává zásadním tématem nejen pro projektanty a architekty, ale i pro odborníky v oblasti stavební fyziky a požární prevence. Současná legislativa v České republice se touto problematikou zatím zabývá pouze okrajově, což zvyšuje riziko při použití hořlavých materiálů, jako je dřevo, v konstrukcích fasád. Cílem tohoto článku je analyzovat chování plamene v různých variantách provětrávaných fasádních systémů s dřevěným obkladem, se zaměřením na faktory ovlivňující šíření požáru a výšku plamene, a přispět tak k větší bezpečnosti dřevostaveb v kontextu moderní architektury [3-6].

2 POPIS EXPERIMENTÁLNÍHO MĚŘENÍ

Cílem projektu bylo experimentálně analyzovat vliv šířky dutiny a úpravy vnitřního povrchu na šíření plamene v provětrávané fasádě z dřevěných palubek prostřednictvím středněrozměrových zkoušek. Hlavním zkoumaným parametrem byla výška plamenů v dutině fasády, přičemž dílčí cíle zahrnovaly měření teplot uvnitř dutiny, sledování tepelného výkonu.

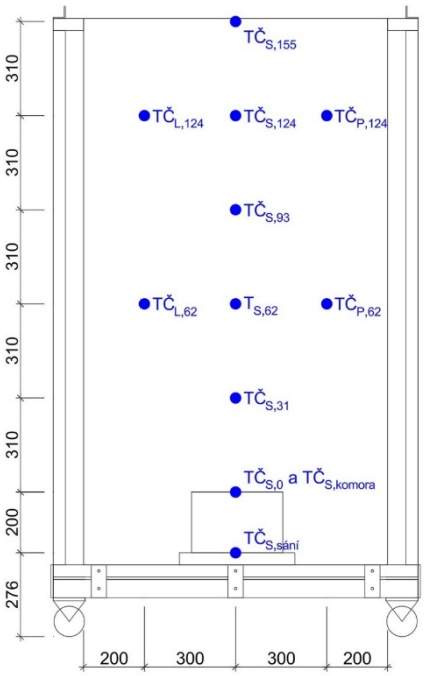
Experimenty vycházely ze švédského výzkumu, který se zabýval vlivem šířky dutiny na výšku plamenů. Se zmenšující se šířkou dutiny dochází ke zvětšení výšky plamenů. Tento jev byl experimentálně prokázán na zařízení, které se skládalo ze dvou nehořlavých desek a hořáku [3].

2.1 ZKUŠEBNÍ ZAŘÍZENÍ

Zařízení sestávalo ze spalovací komory, nehořlavé desky a předstěny s nastavitelnou vzduchovou mezerou.

Limity SBI testu byly stanoveny na tepelný výkon 350 kW a teplotu v potrubí do 400 °C. Pro měření teploty bylo použito 11 termočlánků rovnoměrně rozmístěné v dutině (viz. Obrázek 1), na vermikulitové desce ve spalovací komoře a na vnějším povrchu zkušebního vzorku. Kamerový záznam zachycoval chování plamene, jeho výšku a změny během testu.

Komora SBI testu bylo upraveno pro zajištění optimálních podmínek pro zkoušky, včetně modifikace plynového rozvodu a přidání odnímatelných částí pro usnadnění umístění vzorků. Experimentální měření byla dokumentována videokamerou a zaznamenávána pomocí termočlánků a měřícího zařízení ALMEMO 5690-2.



Obrázek 5, Schéma umístění termočlánků

2.2 VZORKY ZKUŠEBNÍHO MATERIÁLU

Vzorky tvořily smrkové palubky (tloušťka 19 mm, výška 121 mm) upevněné k ocelovému rámu a doplněné vermikulitovou deskou pro snížení tepelného namáhání. Povrch palubek byl ponechán bez úpravy, upraven opálením nebo ošetřen nátěrem z vodního skla. Neošetřený vzorek představoval základní referenční materiál. U opáleného povrchu byla použita japonská metoda „Shou-sugi-ban“, při níž došlo k řízenému opálení povrchu bez následného kartáčování a olejové impregnace, čímž byl simulován nedokonale upravený povrch. Třetí varianta s nátěrem z vodního skla vycházela z běžně dostupné ochrany dřeva proti hoření, přičemž její účinnost byla zkoumána v porovnání s ostatními vzorky.

Vzorky byly voleny tak, aby nebyly ovlivněny dalšími prvky fasády, jako jsou izolace či fólie. Zvolené šířky dutin odpovídaly běžným hodnotám v praxi (20–100 mm), přičemž 60 mm představovalo střední hodnotu. Průměrná vlhkost palubek byla stanovena na 11 %.

Obrázek 6, Zkušební vzorky před měřením (zleva bez povrchové úpravy, opálený, nátěr vodního skla)

2.3 PRŮBĚH MĚŘENÍ

Experimentální měření zahrnovalo 13 požárních zkoušek, přičemž jedna byla provedena bez předstěny a ostatní s reálnou simulací provětrávané fasády. Testovány byly dutiny o šířce 20 mm, 60 mm a 100 mm se zkušebními vzorky z vermikulitové desky, palubek bez úpravy, s opáleným povrchem a s nátěrem z vodního skla.

Před každým měřením bylo do spalovací komory umístěno palivo tvořené dřevěnými hranolky (2 ks 250 x 20 x 15 mm a 16 ks 200 x 20 x 18 mm) o hmotnosti 0,72 - 0,75 kg. K urychlení rozhořívání byl použit podpal z dřevitých provazců napuštěných parafinem. Palivo mělo průměrnou vlhkost 8 % u hranolků 250 mm a 15 % u hranolků 200 mm. Každé měření trvalo 15 minut, po 15 minutě bylo měření přerušeno a vzorky uhašeny. Tabulka 1 uvádí seznam jednotlivých měření.

3 VÝSLEDKY

Tato kapitola se zaměřuje na analýzu naměřených dat, která charakterizují výšku plamene, průběh teplot a tepelný výkon během experimentálních požárních zkoušek. Hodnocení těchto parametrů umožňuje lépe porozumět dynamice šíření plamene v dutině provětrávané fasády a vlivu jednotlivých faktorů, jako je šířka dutiny či povrchová úprava materiálu. Výsledky poskytují klíčové informace pro posouzení požární bezpečnosti fasádních systémů.

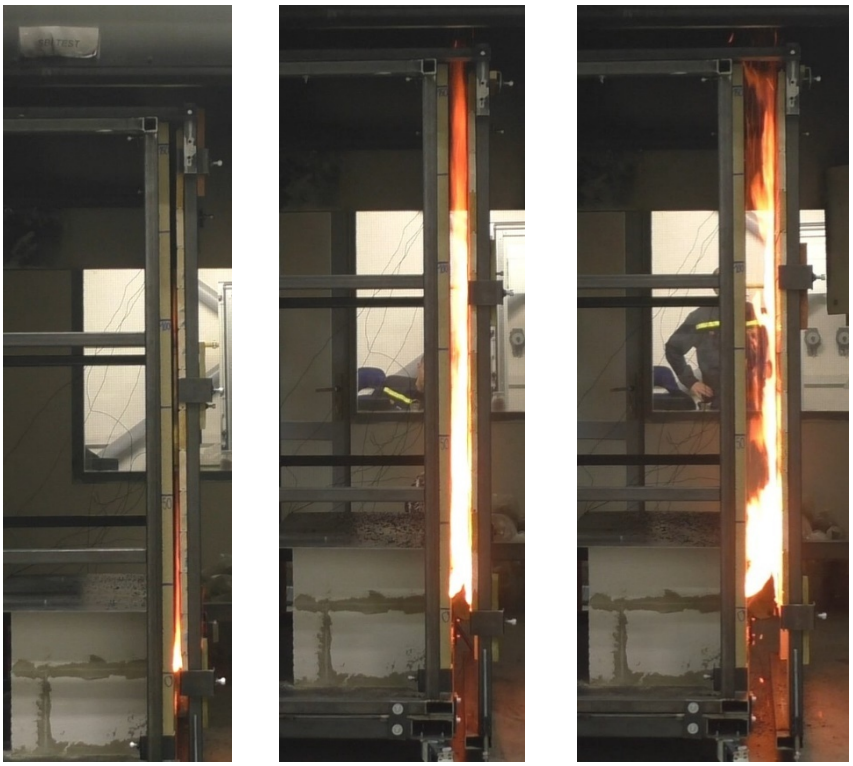
3.1 VÝŠKY PLAMENE

Výška plamenů se lišila v závislosti na šířce dutiny. Při šířce 20 mm byly plameny nejmenší a nejvíce pulsovaly kvůli omezenému přístupu vzduchu, přičemž po vyhoření paliva v komoře hoření v dutině probíhalo s nižší intenzitou.

Při šířce 60 mm dosahovaly plameny maximální výšky a vyplňovaly celý prostor dutiny. U dutiny 100 mm plameny prostor nevyplňovaly a přilnuly k povrchu palubek. Po vyhoření paliva docházelo u dutin 60 mm a 100 mm k samovolnému uhasínání vzorků. Obecně nejmenší výšku plamenů měly vermikulitové desky, následovaly palubky s nátěrem z vodního skla, palubky s opáleným povrchem a největší výšky dosahovaly palubky bez povrchové úpravy. Výsledky potvrzují rozdílné chování plamenů v závislosti na šířce dutiny a typu povrchové úpravy dřeva.

Tabulka 1, Maximální výšky plamenů a doba dosažení

Šířka dutiny [mm]	Povrchová úprava	Čas vyšlehnutí prvních plamenů ze spalovací komory, [min:s]	Maximální výška plamenů, max. 1,5 m, [m]	Čas, kdy plameny dosáhly nejvyšší úrovně, měřeno od začátku experimentu, max. 1,5 m, [min:s]
bez předstěny	bez předstěny	1:47	0,4	6:33
20	bez úpravy	1:38	0,5	6:57
20	opálený povrch	1:23	0,35	6:10
20	nátěr vodního skla	1:26	0,5	6:41
20	vermikulit	1:31	0,4	7:31
60	bez úpravy	0:54	1,5	2:45
60	opálený povrch	0:52	1,5	3:35
60	nátěr vodního skla	0:51	1,5	3:50
60	vermikulit	1:09	0,75	6:01
100	bez úpravy	0:58	1,5	5:20
100	opálený povrch	1:02	1,5	6:50
100	nátěr vodního skla	1:05	1,1	6:25
100	vermikulit	1:29	0,5	7:05



Obrázek 7, Maximální výška plamenů, palubka bez povrchové úpravy (zleva šířka dutiny 20, 600, 100 mm)

3.2 PRŮBĚH TEPLOT

Průběh teplot v dutině se lišil v závislosti na její šířce. U dutiny 20 mm dosahovala maximální teplota 700–800 °C, přičemž zůstávala po většinu zkoušky stabilní a na konci klesla na 600–800 °C. U dutiny 60 mm byla zaznamenána nejvyšší teplota, až 900 °C, s nejstrmějším nárůstem i poklesem, přičemž na konci experimentu klesla na 250–350 °C. U dutiny 100 mm dosahovala teplota maximálně 650–750 °C a na konci experimentu klesla na 100–200 °C. Nejvyšší teploty byly naměřeny u palubek bez povrchové úpravy, zatímco mezi palubkami s opáleným povrchem a s nátěrem z vodního skla nebyly zaznamenány výrazné rozdíly.

3.3 TEPELNÝ VÝKON

Maximální tepelný výkon byl nejvyšší u experimentů s dutinou 60 mm (51,06–64,19 kW) a nejnižší u dutiny 20 mm (19,54–21,87 kW). U dutiny 100 mm dosahoval hodnot 31,00–43,47 kW, zatímco u vermikulitových desek byl výrazně nižší (13,76–15,75 kW). Největší tepelný výkon byl naměřen u palubek bez povrchové úpravy, následovaly palubky s opáleným povrchem a nejnižší hodnoty vykazovaly palubky s nátěrem z vodního skla. Celkové výsledky ukazují, že nejlépe obstály palubky s nátěrem z vodního skla, následované opálenými palubkami, zatímco nejhorší výkon měly palubky bez úpravy. Výsledky však nelze zobecnit, neboť odpovídají podmínkám nízkého tepelného namáhání.

4 ZÁVĚR

Výsledky experimentálního měření ukázaly, že šířka dutiny má zásadní vliv na chování plamene, průběh teplot a tepelný výkon. Nejvyšší plameny byly pozorovány u vzorků s dutinou o šířce 60 mm, kde zároveň docházelo k nejintenzivnějšímu hoření. Při šířce dutiny 100 mm se plameny přilepily k povrchu vzorku a teploty na konci zkoušek byly nižší než u dutiny 60 mm. Nejmenší plameny a nejnižší tepelný výkon byly zaznamenány u vzorků s dutinou 20 mm, kde omezený přístup vzduchu zpomaloval šíření požáru.

Nejvyšších teplot bylo dosaženo u palubek bez povrchové úpravy, zatímco vzorky s opáleným povrchem a nátěrem z vodního skla dosahovaly nižších hodnot. Nejnižší maximální tepelný výkon byl naměřen u vermikulitových desek, které vykazovaly nejlepší požárně bezpečnostní vlastnosti.

Celkově lze konstatovat, že mezi zkoušenými vzorky vykazovaly nejlepší požární odolnost palubky s nátěrem z vodního skla, následované palubkami s opáleným povrchem. Palubky bez povrchové úpravy dosahovaly nejhorších výsledků. Je však nutné brát v úvahu, že získané výsledky odpovídají specifickým podmínkám experimentu a nelze je bez dalšího zobecnit na reálné požární scénáře.

LITERATURA

[1] KRISTOVÁ, M. Statistika výstavby domů za rok 2020 potvrdila rostoucí zájem o dřevostavby. DŘEVO&stavby [online]. 2021 [cit. 2024-12-12]. Dostupné z: https://www.drevoastavby.cz/drevostavby-archiv/doporucujeme/6516-statistika-vystavby-drevostaveb-za-rok-2020

[2] KRISTOVÁ, M. I přes mírný pokles trhu dřevostaveb se v loňském roce stavělo více domů ze dřeva. DŘEVO&stavby [online]. 2022 [cit. 2024-12-12].Dostupnéz:https://www.drevoastavby.cz/drevostavby-archiv/doporucujeme/6998-statistika-admd-2021-podil-drevostaveb-na-trhu

[3] LIVKISS, K., SVENSSON, S., HUSTED, B., VAN HEES, P. Flame Heights and Heat Transfer in Façade System Ventilation Cavities. Fire Technology [online]. 2018, 54(3), 689-713 [cit. 2024-12-12]. ISSN 0015-2684. doi:10.1007/s10694-018-0706-2

[4] ČSN 730802 ed. 2. Požární bezpečnost staveb - Nevýrobní objekty. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2023.

[5] ČSN 730804 ed. 2. Požární bezpečnost staveb - Výrobní objekty. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2023.

[6] ČSN 730810. Požární bezpečnost staveb - Společná ustanovení. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2016.

VLIV ZMĚNY VLASTNICTVÍ NA BEZPEČNOST ZAŘAZENÝCH OBJEKTŮ

Hana Halíčková[1], Michaela Skřížovská[2]

ABSTRAKT

Změna vlastnictví průmyslových objektů spadajících pod zákon o prevenci závažných havárií (PZH) představuje významný faktor ovlivňující bezpečnost provozu. Tento článek poskytuje přehled problematiky změny vlastnictví jako organizační změny, analyzuje legislativní požadavky a identifikuje klíčové aspekty, které by měly být zohledněny při implementaci změn v provozu těchto objektů. Výstupy článku mají sloužit jako informační podklad pro tvorbu praktických nástrojů a pokynů k řízení změn vlastnictví v souladu s požadavky na bezpečnostní dokumentaci a prevenci havárií.

Klíčová slova:
Prevence závažných havárií, bezpečnost, SEVESO, vlastník, změna vlastnictví.

ABSTRACT

The change of ownership of industrial facilities covered by the Prevention of Major Accidents Act is a significant factor affecting the safety of operations. This article provides an overview of the issue of change of ownership as an organisational change, analyses the legislative requirements and identifies key aspects that should be considered when implementing changes in the operation of these facilities. The findings of the paper are intended to inform the development of practical tools and guidelines for managing ownership changes in accordance with safety documentation and accident prevention requirements.

Key words:
Prevention of major accidents, safety, SEVESO, owner, change of ownership.

1 Ing. Hana Halíčková, VŠB-TUO, Fakulta bezpečnostního inženýrství, Lumírova 630/13, 700 30 Ostrava – Výškovice, +420 596 992 835, hana.halickova@vsb.cz
2 Ing. Michaela Skřížovská, Ph.D., VŠB-TUO, Fakulta bezpečnostního inženýrství, Lumírova 630/13, 700 30 Ostrava – Výškovice

1 ÚVOD

Změna vlastníka nebo provozovatele objektu zařazeného do skupiny A nebo B podle legislativy (tj. směrnice evropského parlamentu a rady 2012/18/EU o kontrole nebezpečí závažných havárií s přítomností nebezpečných látek a o změně a následném zrušení směrnice Rady 96/82/ES, SEVESO DIREKTIVA III (Seveso III)) představuje organizační změnu, která může mít zásadní dopady na bezpečnost provozu a řízení rizik. Převod vlastnictví, změna provozovatele nebo restrukturalizace společnosti často vedou ke změnám v odpovědnostech, organizační kultuře, kultuře bezpečnosti a řízení rizik, což může ovlivnit kontinuitu systémů řízení bezpečnosti [1].

V rámci prevence závažných havárií (PZH) je nezbytné, aby změna vlastnictví probíhala s ohledem na zachování bezpečnostních standardů a legislativních požadavků. Evropská směrnice Seveso III a její implementace v českém právním prostředí (Zákon č. 224/2015 Sb., o prevenci závažných havárií a příslušné prováděcí předpisy) obsahují požadavky na řízení organizačních změn, ale nestanovují konkrétní požadavky na změnu vlastnictví. To může vést k nejasnostem v praxi, především pokud jde o přenos odpovědnosti a bezpečnostní dokumentaci [2].

Cílem tohoto článku je analyzovat přístup ke změně vlastnictví v kontextu prevence závažných havárií a zhodnotit legislativní požadavky spojené s touto změnou. Na základě dostupných informací, identifikovaných výzev a praktických potřeb průmyslu dojde k formulování doporučení a vytvoření podkladu pro zpracování praktických nástrojů, které by umožnily efektivní a bezpečné provedení změny vlastníka průmyslových objektů.

2 ZMĚNA VLASTNICTVÍ JAKO SPECIFICKÁ ORGANIZAČNÍ ZMĚNA

Organizační změny mohou mít různé podoby – od restrukturalizace v rámci společnosti po změnu vlastnictví celého podniku nebo jeho části. V kontextu průmyslových podniků regulovaných Seveso III direktivou představuje změna vlastníka zásadní událost, která ovlivňuje strategické řízení bezpečnosti a plnění legislativních požadavků [3].

Změna vlastníka podniku patří mezi organizační změny, které mohou mít zásadní dopad na řízení bezpečnosti. I přesto nebývá systematicky zohledňována v bezpečnostní dokumentaci jako součást řízení změn. OECD (2023) ve svých základních principech pro prevenci chemických havárií upozorňuje, že změna vlastnictví je významným faktorem, který může zvýšit riziko vzniku závažné havárie, a proto by měla být vyhodnocována z hlediska bezpečnosti. Nový vlastník totiž často přináší jinou bezpečnostní kulturu, přístup k řízení rizik nebo změny v odpovědnostech, což může ovlivnit připravenost podniku na mimořádné události.

OECD (2018) proto doporučuje přistupovat ke změně vlastníka jako k vícestupňovému procesu, který zahrnuje různé úrovně rizika, od fáze přípravy podniku k prodeji až po ustálení nového stavu po převzetí.

2.1 TYPY PŘEMĚN ORGANIZACÍ

Česká legislativa rozlišuje několik typů přeměn organizací (změny vlastnictví):

- fúze (sloučením nebo splynutím),
- rozdělení (např. rozštěpení nebo odštěpení),
- převod jmění na společníka,
- změnu právní formy a
- přeshraniční přemístění sídla [4].

Každá z těchto forem může přinášet specifická rizika, která je třeba vyhodnotit z hlediska dopadu na bezpečnostní procesy. Z hlediska provozní bezpečnosti je zvláště důležité pečlivě posoudit situace, kdy dochází ke sloučení nebo rozdělení společnosti nebo když dochází převodu obchodního podílu na jinou osobu (např. v rámci dědického řízení) mimo stávající společníky – tato forma změny může znamenat vstup vlastníka bez zkušeností s řízením rizik v nebezpečném provozu [3].

2.2 PRŮZKUM V MORAVSKOSLEZSKÉM KRAJI

Význam této změny dokládá i analýza podniků v Moravskoslezském kraji, kde u více než 80 % z 22 aktuálně zařazených podniků do skupin A nebo B podle zákona o PZH došlo minimálně jednou ke změně vlastníka [5]. Z průzkumu dále vyplynulo že u více než poloviny podniků došlo k fúzi nebo rozdělení (některé podniky podstoupily obě tyto změny). To potvrzuje, že změna vlastnictví je běžným jevem a měla by být zohledněna jako potenciální rizikový faktor v rámci systému řízení bezpečnosti.

2.3 ODPOVĚDNOST ZA OBLAST PZH

Za plnění povinností v oblasti prevence závažných havárií (PZH) je podle zákona odpovědný provozovatel [6]. V praxi jsou specifické úkoly a odpovědnosti provozovatele často delegovány na osoby důležité z hlediska bezpečnosti (např. vedoucí výroby, technický ředitel, manažer BOZP, odborný garant pro PZH). Tato delegace však nezbavuje vlastníka odpovědnosti, ale umožňuje efektivnější řízení rizik za předpokladu splnění zásadních kompetencí.

3 DOPADY ZMĚNY VLASTNICTVÍ NA PZH

Organizační změny patří mezi faktory, které mohou významně přispět ke vzniku závažných havárií. Ačkoliv nejsou tak časté jako technické změny, jejich dopady bývají podceňovány. Podle analýz představují přibližně 5,4 % případů selhání řízení změn, často v souvislosti s personálními změnami, reorganizací nebo výměnou vedení. Důsledkem bývá ztráta odbornosti, přetížení personálu, oslabení bezpečnostní kultury a selhání systému řízení bezpečnosti [7].

Typickým příkladem je havárie rafinerie BP v Texas City z roku 2005, při níž zahynulo 15 lidí a více než 180 bylo zraněno. Následky havárie ilustruje obrázek 1. Příčinou bylo zanedbání modernizace po změně vlastnictví, škrty v rozpočtu a snížení počtu zaměstnanců. Vedení nedávalo důraz na procesní bezpečnost, což spolu s organizačními problémy a slabým školením vedlo ke katastrofě. [8] Případ ukazuje, jak zásadní dopady může mít změna vlastnictví při zanedbání řízení rizik.

Obrázek 8 Následky havárie v texaské rafinérii BP [9]

V rámci studie byly identifikovány klíčové zdroje rizik související se změnou vlastnictví. Mezi nimi například ztráta firemní paměti zejména v souvislosti s odchodem zkušených zaměstnanců z pozic zásadních pro řízení PZH neb narušení bezpečnostní kultury, ke které dochází zejména při fúzích a akvizicích, kdy dochází ke střetávání firemních kultur [7].

4 PROBLEMATIKA ZMĚNY VLASTNICTVÍ V ČR

Tato studie slouží jako základ pro vytvoření praktických nástrojů a pokynů pro bezpečné provedení změny vlastnictví podniků na území ČR. Proto byla provedena zejména analýza legislativních požadavků v českém právním prostředí a rovněž byl proveden průzkum v praxi pro získání informací o omezeních a potřebách podniků a příkladu dobré praxe.

4.1 LEGISLATIVNÍ RÁMEC

Základním legislativním dokumentem vztahujícím se k prevenci závažných havárií a provozováním zařízení s nebezpečnými látkami je směrnice Seveso III [10]. Směrnice stanovuje rámcové požadavky na evropské úrovni. Členským státům ukládá povinnost zajistit, aby provozovatelé přijímali veškerá nezbytná opatření k prevenci závažných havárií (PZH), včetně řízení změn, které se mohou dotýkat organizační struktury a vlastnictví. Článek 11 této směrnice specifikuje povinnost přehodnocení a aktualizace bezpečnostní dokumentace v případě změn, jež by mohly ovlivnit riziko vzniku závažné havárie. Přestože změna vlastníka není výslovně upravena, jakékoli významné změny musí být včas oznámeny příslušnému orgánu [10].

V českém právním prostředí jsou požadavky směrnice Seveso III implementovány zákonem č. 224/2015 Sb., o prevenci závažných havárií [6] a prováděcími právními předpisy. Vyhláška č. 227/2015 Sb. [11] specifikuje obsah bezpečnostní dokumentace, jejíž součástí je SŘB. Povinností provozovatelů je uvést v SŘB informace o postupech v procesu řízení změn v oblastech uvedených na obrázku 2. Obrázek 3 pak znázorňuje popis oblasti řízení změn v objektu. Jedná se pouze o rámcový výčet informací, které musí být uvedeny v popisu SŘB. Jde však jen o povinnost uvedení informací těchto informací, a ne přímo o povinnost provádění uvedených kroků. Zejména odborné posouzení změny by mělo být legislativně vyžadováno.

Obrázek 9 Tematické okruhy SŘB (podle [11])

Obrázek 10 Tematické okruhy pro oblast řízení změn (podle [11])

S otázkou vlastnictví souvisí i zákon č. 37/2021 Sb., o evidenci skutečných majitelů [12], který ukládá povinnost identifikovat osoby s rozhodovacím vlivem. Tato informace je důležitá zejména pro přiřazení odpovědnosti za řízení rizik spojených s provozem zařízení.

4.2 POZNATKY Z PRAXE

Za účelem doplnění teoretické analýzy o pohled z praxe byla provedena kombinace kvalitativního a kvantitativního sběru dat. V rámci rozhovoru s jedním z provozovatelů objektu podléhajícího zákonu o prevenci závažných havárií byly zjišťovány zkušenosti s procesem změny vlastnictví, včetně toho, jak je tato změna reflektována v systému řízení bezpečnosti a bezpečnostní dokumentaci. Současně bylo provedeno orientační dotazníkové šetření mezi vybranými podniky zařazenými podle zákona č. 224/2015 Sb., jehož cílem bylo identifikovat míru připravenosti na změnu vlastnictví, potřeby podniků a případné nedostatky v aplikační praxi. Doplněním této analýzy byl také příklad dobré praxe ze společnosti v Moravskoslezském kraji, kde právě probíhala příprava na změnu vlastnictví části podniku.

Ze sběru dat vyplynulo, že změna vlastnictví není v praxi systematicky chápána jako významná změna s potenciálním dopadem na bezpečnost provozu. U většiny podniků chybí konkrétní interní postupy či pokyny, jak takovou změnu bezpečně řídit, zejména pokud dochází i ke změně organizační struktury. Provozovatelé zároveň uváděli nejistotu ohledně legislativních požadavků, především v tom, kdy a jak aktualizovat bezpečnostní dokumentaci. Potvrzena byla potřeba metodické podpory a praktických nástrojů, které by změnu vlastnictví systematicky zahrnuly do procesu řízení změn a přispěly ke zlepšení kultury bezpečnosti při přechodu mezi subjekty.

5 ZÁVĚR

Změna vlastnictví zařazených objektů představuje významnou organizační změnu s potenciálně zásadním dopadem na bezpečnost provozu. Provedený průzkum ukazuje, že se jedná o běžný typ změny, kterým prochází většina podniků. Při takové změně je klíčové je zajistit kontinuitu v řízení bezpečnosti, přenos odpovědností, zachování firemní paměti a kultury bezpečnosti.

Přestože legislativa v oblasti PZH stanovuje rámcové požadavky a klade důraz na řízení změn, změna vlastnictví není přímo řešena. Z provedené analýzy a průzkumů vyplývá, že chybí specifické metodické pokyny. To v praxi vede k nejasnostem a podceňování rizik souvisejících se změnou vlastnictví. V podnicích pak často chybí systematické přístupy a interní procesy pro řízení změn včetně změny vlastnictví (např. mechanismy pro přenos klíčových znalostí).

Na základě těchto zjištění budou vyvíjeny praktické nástroje a pokyny určeny především pro provozovatele zařazených objektů, pracovníky zodpovědné za oblast bezpečnosti (např. manažery BOZP, technické ředitele, odborné garanty PZH) a také pro vlastníky a vedení podniků, kteří rozhodují o majetkových a organizačních změnách. Současně mohou sloužit jako podklad

pro kontrolní a dozorové orgány, které posuzují naplnění zákonných povinností při provozních změnách.

PODĚKOVÁNÍ

Tento příspěvek byl vytvořen s podporou Vysoké školy báňské – Technické univerzity Ostrava, Fakulty bezpečnostního inženýrství.

Výzkum byl proveden v rámci dílčí části (Studie vlivu změny provozovatele objektu na PZH) projektu TAČR SS02030008 Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH).

LITERATURA

[1] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT [OECD], 2017. *Corporate governance for process safety: Guidance for senior leaders in high hazard industries*, Series on Chemical Accidents, OECD Publishing, Paris. Dostupné z: https://doi.org/10.1787/9789264274846-en [cit. 2025-03-18].

[2] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT [OECD], 2018. *Guidance on Change of Ownership in Hazardous Facilities*. Environment, Health and Safety, Environment Directorate, OECD. Dostupné z: https://www.oecd.org/chemicalsafety/chemical-accidents/oecd-guidance-on-change-of-ownership-in-hazardous-facilities.pdf [cit. 2025-03-18].

[3] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT [OECD], 2023. *OECD Guiding Principles for Chemical Accident Prevention, Preparedness and Response - Third Edition*, Series on Chemical Accidents. Paris: OECD Publishing. Dostupné z: https://doi.org/10.1787/162756bf-en [cit. 2025-03-18].

[4] Zákon č. 125/2008 Sb., o přeměnách obchodních společností a družstev. In: *Sbírka zákonů ČR*. Částka 40. [cit. 2025-03-20].

[5] MINISTERSTVO SPRAVEDLNOSTI ČR. *Veřejný rejstřík a Sbírka listin*. Online. Praha: Ministerstvo spravedlnosti. Dostupné z: https://or.justice.cz. [cit. 2025-03-20].

[6] Zákon č. 224/2015 Sb. o prevenci závažných havárií způsobených vybranými nebezpečnými chemickými látkami nebo chemickými směsmi a o změně zákona č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů, (zákon o prevenci závažných havárií). In: *Sbírka zákonů ČR*. Částka 93. [cit. 2025-03-20].

[7] HAN SIONG, P.; CHIN, K.Y.; BAKAR, H.T.A.; LING, C.H.; KIDAM, K. et al., 2017. The contribution of management of change to process safety accident in the chemical process industry. *Chemical Engineering Transactions*. Roč. 56, s. 1363-1368. ISSN 2283-9216.

[8] KLETZ, Trevor a AMYOTTE, Paul, 2019. *What Went Wrong?* Sixth Editon. Elsevier. ISBN 978-0-12-810539-9.
[9] U.S. CHEMICAL SAFETY BOARD [CSB], 2007. *Investigation Report - Refinery Explosion and Fire: BP Texas City, Texas, March, 2005*. Online. Dostupné z: https://www.csb.gov/file.aspx?DocumentId=5596. [cit. 2025-03-27].
[10] Směrnice Evropského parlamentu a Rady 2012/18/EU ze dne 4. července 2012 o kontrole nebezpečí závažných havárií s přítomností nebezpečných látek a o změně a následném zrušení směrnice Rady 96/82/ES Text s významem pro EHP. In: *Úřední věstník Evropské unie*.
[11] Vyhláška č. 227/2015 Sb., o náležitostech bezpečnostní dokumentace a rozsahu informací poskytovaných zpracovateli posudku. In: *Sbírka zákonů ČR*. Částka 94.
[12] 2021. Zákon č. 37/2021, o evidenci skutečných majitelů. In: *Sbírka zákonů ČR*. Částka 17.

BEZPEČNOST V KOLABORATIVNÍ ROBOTICE

Kristýna Hamříková[1]

ABSTRAKT

Kolaborativní roboty neboli koboty se vyznačují především svou spoluprací s člověkem bez přítomnosti takové míry rizika, jakou představují průmyslové roboty. Míra rizika u kobotů je výrazně nižší než u průmyslových robotů, ovšem není nulová, proto je důležité provádět posouzení rizik na pracovišti správně a důkladně. Článek bude zaměřen na představení kobotů, rizik při jejich použití a vhodná bezpečnostní opatření. Vzhledem k absenci předepsaných technik posuzování bezpečnosti kolaborativních robotů bude pozornost věnována vhodným technikám analýzy rizik při procesní bezpečnosti (HAZOP-UML, STPA a Úkolové metody hodnocení rizik). Všechny tyto techniky jsou nejčastěji využívány pro tyto kolaborativní systémy.

Klíčová slova:
Koboty, techniky, posouzení rizik, rizika, nebezpečí.

ABSTRACT

Collaborative robots, or cobots, are characterized primarily by their cooperation with humans without the presence of such a level of risk as industrial robots. The level of risk in cobots is significantly lower than in industrial robots, but it is not zero, which is why it is important to carry out a risk assessment in the workplace correctly and thoroughly. The article will focus on introducing cobots, the risks in their use and appropriate safety measures. Due to the absence of prescribed techniques for assessing the safety of collaborative robots, attention will be paid to appropriate risk analysis techniques for process safety (HAZOP-UML, STPA and Task-based risk assessment methods). All of these techniques are most often used for these collaborative systems.

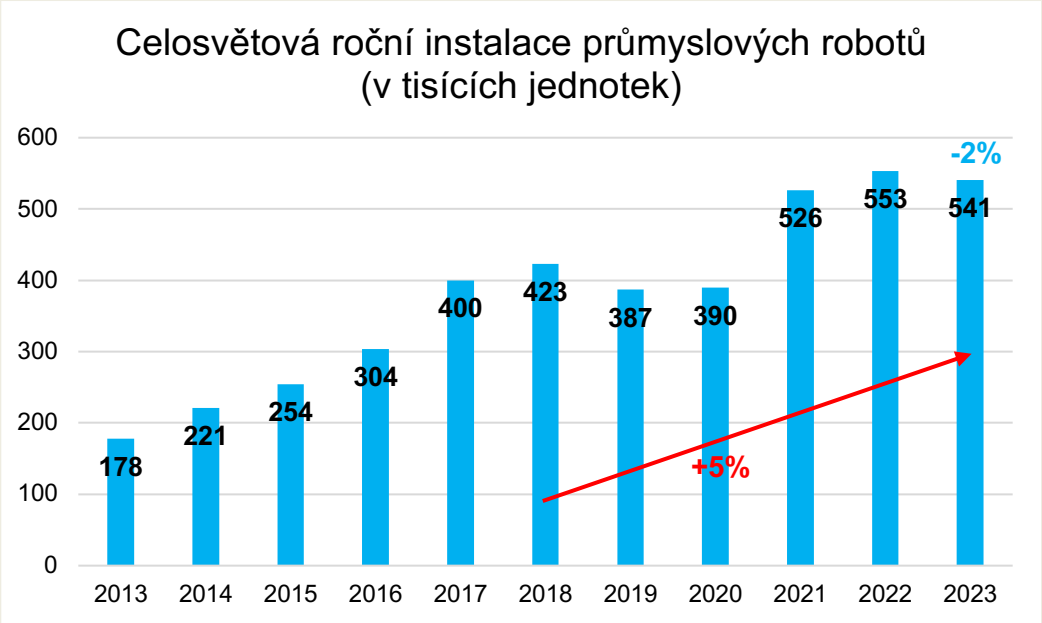
Key words:
Cobots, techniques, risk assessment, risks, dangers.

1 Kristýna Hamříková Ing., Lumírova 630/13, 700 30 Ostrava-jih-Výškovice,
+420 733 527 114, kristyna.hamrikova@vsb.cz

ÚVOD

Kolaborativní robot neboli kobot, je typem robotu určeného ke spolupráci s lidmi. Koboty jsou vybaveny pokročilými senzory, sofistikovanými řídicími systémy a bezpečnostními prvky, které jim umožňují pracovat po boku lidí efektivně a většinou bez významných rizik. Na rozdíl od tradičních průmyslových robotů, které jsou z bezpečnostních důvodů často od lidí odděleny bariérami nebo ploty, jsou koboty navrženy tak, aby sdílely stejný pracovní prostor s lidskými pracovníky. Tento způsob umožňuje snadnou a efektivní spolupráci. Hlavním cílem kobotů je podpora lidských schopností, zvýšení produktivity, zlepšení efektivity a zajištění bezpečnějšího a flexibilnějšího pracovního prostředí [1].

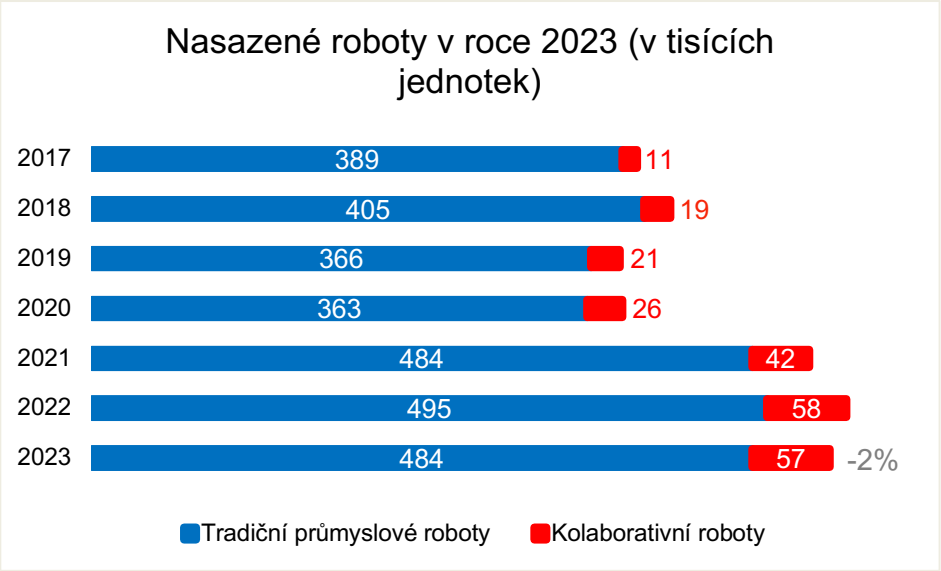
Využívání průmyslových robotů i kobotů není pouze průmyslový trend, ale žádoucím krokem z pohledu konkurenceschopnosti [1]. Mezinárodní federace robotiky (dále jen IFR), poskytla statistická data celosvětových instalací robotů za rok 2023, která jsou uvedena v grafu 1.



Graf 1 Data roční instalace robotů [2]

Rok 2022 představoval klíčový rok, neboť došlo k rekordním instalacím robotů na světě. Jednalo se o 553 tisíc instalací. Za rok 2023 došlo k mírnému poklesu oproti roku 2022, ale pouze o 2 % [2]. Ovšem tento pokles nepředstavuje žádný významný signál naznačující, že by v budoucnu měl zájem o průmyslové roboty a koboty klesat.

IFR sestavuje i roční statistiku nasazených kobotů, která zahrnuje i průmyslové roboty, které jsou navrženy a určeny pro kolaborativní použití v souladu s ISO 10218-1. V roce 2023 představoval počet nově nasazených kolaborativních robotů 57 tisíc kusů. Což představovalo 10,5 % z celkového počtu instalovaných průmyslových robotů viz graf 2 [2].



Graf 2 Roční nasazení robotů [2]

TYPY KOLABORATIVNÍCH ROBOTŮ

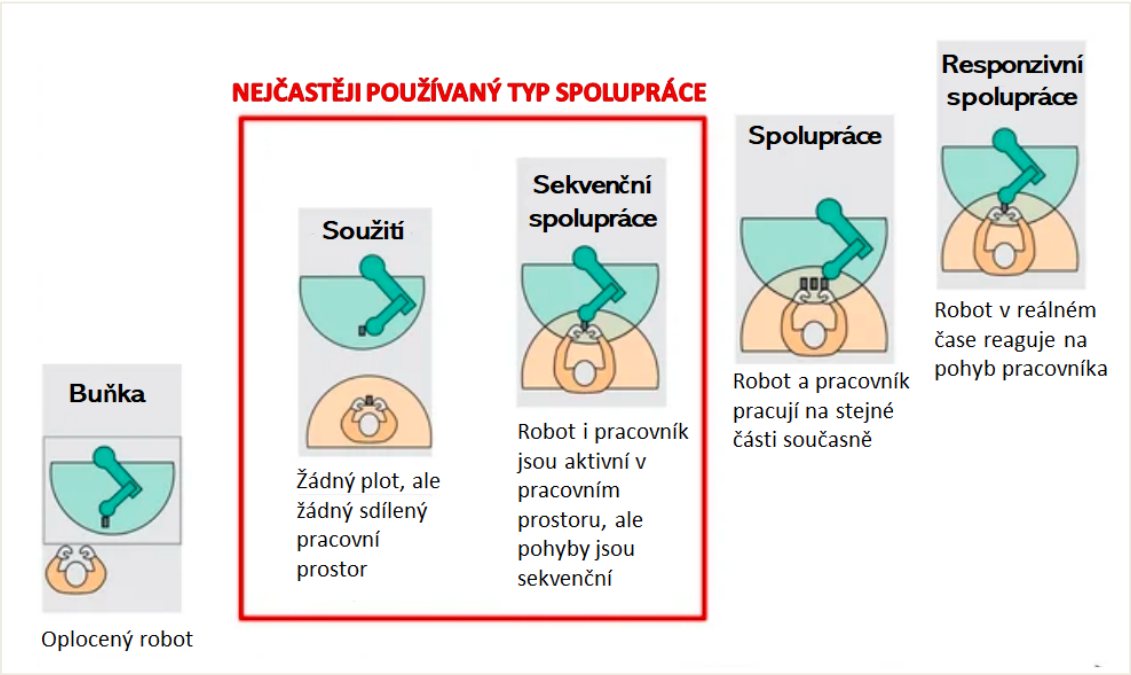
IFR definuje dva typy robotů určených pro spolupráci. Jedna skupina zahrnuje roboty navržené pro kolaborativní použití, které splňují normu ISO 10218-1, která specifikuje požadavky a pokyny pro inherentně bezpečnou konstrukci, ochranná opatření a informace pro použití průmyslových robotů. Druhá skupina zahrnuje roboty určené pro kolaborativní použití, které nesplňují požadavky normy ISO 10218-1. To neznamená, že tyto roboty nejsou bezpečné. Mohou se řídit různými bezpečnostními normami, např. národními nebo vnitrostátními [3].

Existují značné rozdíly v typech kolaborativních robotů splňujících výše uvedené specifikace a úroveň kontaktu mezi robotem a pracovníkem v kolaborativních aplikacích. Na jednom konci technického spektra jsou tradiční průmyslové roboty pracující v odděleném pracovním prostoru, do kterého mohou pracovníci pravidelně vstupovat, aniž by museli předem vypínat napájení robota a zabezpečit výrobní buňku. Pracovní prostor robota může být vybaven senzory, které detekují pohyb člověka a zajišťují, aby robot pracoval velmi nízkou rychlostí nebo se zastavil, když je pracovník v určeném pracovním prostoru. Na druhém konci spektra jsou průmyslové roboty navržené speciálně pro práci po boku lidí ve sdíleném pracovním prostoru. Tyto roboty, často označované jako "koboty", jsou navrženy s řadou technických vlastností, které zajišťují, že nezpůsobí újmu, když se pracovník dostane do přímého kontaktu, ať už úmyslně nebo náhodou. Mezi tyto vlastnosti patří lehké materiály, zaoblené kontury, polstrování, tzv. "kůže" (polstrování se zabudovanými senzory) a také senzory na základně nebo kloubech robota, které měří a řídí sílu a rychlost a zajišťují, aby v případě kontaktu nepřekročily definované prahové hodnoty stanovené v normě ISO/TS 15066. Tyto hodnoty jsou definovány pro různé části lidského těla, aby nedošlo k poranění [3], [4].

Koboty se dále rozdělují podle umístění referenčního rámce na několik tříd:

- pevné koboty: stacionární roboty vhodné pro úkoly, jako je montáž nebo manipulace s materiálem;
- mobilní koboty: roboty schopné pohybu v rámci pracovního prostoru, často využívané v logistice nebo zdravotnictví;
- hybridní koboty: Kombinují vlastnosti stacionárních a mobilních kobotů, což umožňuje jejich univerzální použití.

Kromě těchto kategorií lze koboty dále klasifikovat podle kapacity užitečného zatížení, způsobu programování nebo stupně autonomie [4].



Obrázek 11 Typy spoluprací člověk – robot [5]

RIZIKA A NEBEZPEČÍ

Při hodnocení rizik spojených s kolaborativními roboty je nezbytné brát v úvahu nejen samotného robota, ale také celé pracovní prostředí, ve kterém funguje. Kromě samotného robota, jeho chapadel, efektorů či nástrojů, je nutné věnovat pozornost i dalším prvkům v pracovním prostoru (buňce), jako jsou kabely, fixační přípravky nebo manipulované objekty apod. Na rozdíl od tradičních průmyslových robotů, kde je interakce s člověkem minimální, je u kobotů nutné analyzovat a hodnotit předvídatelné i záměrné kontakty mezi člověkem a robotem. To zahrnuje určení typu, četnosti a lokace kontaktu na lidském těle [6].

Podle normy ISO/TS 15066 je kolaborativní robot bezpečný pouze tehdy, pokud kontakt s ním nezpůsobuje bolest. Pokud dochází k bolestivým, ale

neškodným kontaktům, jejich četnost musí být přísně regulována. V případech, kdy existuje riziko závažného poranění, musí být implementována další bezpečnostní opatření, případně kobot nelze v daném procesu použít. Zvláštní důraz musí být kladen na riziko kontaktu s horní částí těla, zejména hlavou a krkem. Pokud pracovní proces vyžaduje expozici těchto částí těla, musí obsluha používat ochrannou přilbu a obličejový štít. Dále je nezbytné zajistit, aby žádná část těla nebyla vystavena riziku skřípnutí mezi pohyblivými částmi robota nebo mezi robotem a okolními objekty, jako jsou stěny nebo pracovní desky [6], [7].

Seznam nebezpečí, která mohou roboty a robotické systémy představovat pro člověka jsou uvedeny v seznamu významných nebezpečí v normě ČSN EN ISO 10218 v příloze A a dělí se do následujících skupin:

- Mechanická nebezpečí;
- Elektrická nebezpečí;
- Tepelná nebezpečí;
- Nebezpečí hluku;
- Nebezpečí vibrací;
- Nebezpečí záření;
- Nebezpečí materiálu/látky;
- Ergonomická nebezpečí;
- Nebezpečí spojená s environmentem, ve kterém je stroj používán;
- Kombinace nebezpečí [8].

Další rizika souvisejí s kybernetickou bezpečností, kdy hrozí neoprávněný přístupu do systému kobota. Může dojít k nebezpečné manipulaci s funkcemi kobota, což může ohrozit bezpečnost operátora i výrobního procesu. Dalším klíčovým aspektem je ochrana osobních údajů – roboty vybavené senzory a kamerami mohou shromažďovat citlivé informace, což může představovat hrozbu pro soukromí zaměstnanců. Řešení těchto problémů vyžaduje komplexní přístup, který zahrnuje např. technická opatření v podobě zabezpečení softwaru, šifrování dat a pravidelné aktualizace [6].

Mezi potenciální rizika spojená s využíváním kobotů při spolupráci lze zařadit např.:

Selhání nebo neočekávaná změna „chování“ kobota. K této situaci může dojít např. v případě selhání důležitých čidel, softwarových systémů a algoritmů nebo kybernetického útoku. Toto selhání může vést ke kolizím s pracovníky a způsobit jim zranění [9].

Kolize a neúmyslný kontakt s pracovníkem. Ke kolizím může dojít při nečekávaném pohybu pracovníka nebo kobota ve společném pracovním prostoru. I přes to, že jsou koboty vybaveny senzory pro detekci apod. k těmto situacím může dojít. Proto je důležité, aby byl kobot vždy správně a individuálně naprogramovaný a pracovníci byli proškoleni [9].

Psychosociální rizika. Příkladem je studie [10], která se zabývala vlivem kobota na psychiku člověka a uvádí experimentální studii zaměřenou na

psychologickou (primární a sekundární hodnocení), fyziologickou (srdeční frekvence) a stresovou reakci na různé režimy kobotů u operátorů.

TECHNIKY POSOUZENÍ RIZIK

V oblasti procesní bezpečnosti doposud neexistuje žádná jednotná technika, která by se pro posouzení rizik kobotů využívala, což potvrzují např. tyto studie [12] a [13]. Posouzení rizik v procesní bezpečnosti se v případě kobotů, provádí prostřednictvím normy ČSN EN ISO 31010. Tato norma obsahuje mnoho metodik a technik pro identifikaci, analýzu a hodnocení rizik, které jsou vhodné pro různé environmenty, objekty, stroje, požadavky a preference.

Podle článku *Risk assessment tools for industrial human-robot collaboration: Novel approaches and practical needs* [11] se pro komplexní posouzení rizik v kolaborativní roobtice využívají nejčastěji tyto následující techniky:

- HAZOP a HAZOP-UML
- STPA
- FMEA
- FTA
- HTA
- Top-down a Bottom-up přístup
- Úkolové metody hodnocení rizik.

Všechny tyto výše uvedené techniky pokrývají jak identifikaci rizik, tak analýzu rizik a jsou vhodné pro použití v různých fázích návrhu kolaborativních robotických systémů.

Nejčasteji využívané techniky hodnocení rizik v kolaborativní robotice se používají tyto techniky:

- QRA
- Matice rizik
- Simulace kolizí a biomechanické testy
- Norma ISO 12100 a ISO/TS 15066 [11].

ZÁVĚR

Pro bezpečnost kolaborativní robotiky je žádoucí vytvořit nástroj/techniku, která pokrývá kompletní proces posouzení rizik. Bude snadný pro implementování do firem a zároveň jednoduchý pro použití v praxi. Dalším problémem je, že stávající techniky málo zohledňují lidské chování – např. nečekané reakce operátora nebo psychologické aspekty jako je únava, stres apod.

Proto vzniká na Fakultě bezpečnostního inženýrství VŠB-TUO laboratoř kolaborativní robotiky, která bude propojovat dva směry, a to funkční a procesní bezpečnost. Díky tomuto propojení dojde k ujasnění důležitosti vzájemného vztahu a spolupráce mezi integrátorem a bezpečnostním technikem při implementaci kobota do pracovního prostředí.

Z výše uvedených důvodů se v rámci své disertační práce a SGS budu zabývat důležitostí spolupráce mezi integrátorem a bezpečnostním technikem, komplexním posouzením rizik funkční i procesní bezpečnosti a vytvořením jednotné metodiky posouzení rizik obou těchto směrů.

LITERATURA

[1] FRANKLIN, Carole S.; DOMINGUEZ, Elena G.; FRYMAN, Jeff D. a LEWANDOWSKI, Mark L. Collaborative robotics: New era of human–robot cooperation in the workplace. Online. Journal of Safety Research. 2020, vol. 74, s. 7. ISSN 0022-4375. Dostupné z: https://doi.org/10.1016/j.jsr.2020.06.013. [cit. 2025-03-10].

[2] INTERNATIONAL FEDERATION OF ROBOTICS. World Robotics: Press Conference 2024. Online. IFR. Frankfurt, 2024. Dostupné z: https://ifr.org/img/worldrobotics/Press_Conference_2024.pdf. [cit. 2025-03-10].

[3] IFR. World Robotics - Industrial Robots. Online. IFR. International Federation of Robotics. C2025. Dostupné z: https://ifr.org/industrial-robots. [cit. 2025-03-10].

[4] TAESI, Claudio; AGGOGERI, Francesco a PELLEGRINI, Nicola. COBOT Applications—Recent Advances and Challenges. Online. Robotics. 2023, vol. 12, no. 3, s. 33. ISSN 2218-6581. Dostupné z: https://doi.org/10.3390/robotics12030079. [cit. 2025-03-10].

[5] Vytvořeno autorem: Ing. Kristýna Hamříková, na základě informací z: IFR. World Robotics – Industrial Robots. Online. IFR. International Federation of Robotics. C2025. Dostupné z: https://ifr.org/industrial-robots. [cit. 2025-03-10].

[6] SAMUE, Filip. BEZPEČNOST V RÁMCI APLIKACE KOLABORATIVNÍCH ROBOTŮ: SAFETY OF COLLABORATION ROBOTS. Bakalářská práce. Brno: VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ, 2024.

[7] ISO. ISO/TS 15066, Technical specification Robots and robotic devices – Collaborative robots. Švýcarsko, 2016.

[8] ÚNMZ. ČSN EN ISO 10218-1, Roboty a robotická zařízení – Požadavky na bezpečnost průmyslových robotů – Část 1: Roboty. Praha, 2012.

[9] Kolaborativní roboti (koboti). BOZP.cz. Výhody, rizika, bezpečnost. Online. BOZP.cz. 2024. Dostupné z: https://www.bozp.cz/aktuality/kolaborativni-roboti-koboti/#kap_2. [cit. 2025-01-06].

[10] POLLAK, Anita; PALIGA, Mateusz; PULOPULOS, Matias M.; KOZUSZNIK, Barbara a KOZUSZNIK, Malgorzata W. Stress in manual and autonomous modes of collaboration with a cobot. Online. Computers in Human Behavior. 2020, roč. 112, s. 8. ISSN 0747-5632. Dostupné z: https://doi.org/10.1016/j.chb.2020.106469. [cit. 2025-01-05].

[11] HUCK, Tom P.; MÜNCH, Nadine; HORNUNG, Luisa; LEDERMANN, Christoph a WURLL, Christian. Risk assessment tools for industrial human-robot collaboration: Novel approaches and practical needs. Online. Safety Science. 2021, vol. 141, s. 9. ISSN 0925-7535. Dostupné z: https://doi.org/10.1016/j.ssci.2021.105288. [cit. 2024-12-12].

[12] HUCK, Tom P.; MÜNCH, Nadine; HORNUNG, Luisa; LEDERMANN, Christoph a WURLL, Christian. Risk assessment tools for industrial human-robot collaboration: Novel approaches and practical needs. Safety Science. 2021, vol. 105288, no. 141, s. 9. ISSN 0925-7535. Dostupné také z: https://doi.org/10.1016/j.ssci.2021.105288.

[13] ZHANG, Ming; XU, Rui; WU, Haitao; PAN, Jia a LUO, Xiaowei. Human–robot collaboration for on-site construction. Automation in Construction. 2023, vol. 104812, no. 150, s. 17. ISSN 0926-5805. Dostupné také z: https://doi.org/10.1016/j.autcon.2023.104812.

COMPARISON OF CONVOLUTIONAL NEURAL NETWORK ARCHITECTURES FOR EFFICIENT FACE RECOGNITION IN SECURITY PRACTICE

Martin Haváček[1]

ABSTRAKT

Táto práca sa zameriava na porovnanie efektivity vybraných konvolučných neurónových sietí (CNN) pri rozpoznávaní tvárí. Experimenty prebiehali na dátovej sade Labeled Faces in the Wild (LFW), pričom boli testované rôzne predtrénované CNN dostupné v prostredí MATLAB. Hodnotila sa presnosť klasifikácie a výpočtová náročnosť jednotlivých sietí. Výsledky ukázali výrazné rozdiely medzi jednotlivými CNN, pričom siete DarkNet-19 a DenseNet-201 dosiahli najvyššiu presnosť. Potvrdilo sa, že presnosť CNN výrazne ovplyvňuje architektúra siete, veľkosť tréningovej sady a zvolené tréningové parametre.

Kľúčové slová:
konvolučné neurónové siete; hlboké učenie; rozpoznávanie tvárí; bezpečnostné aplikácie

ABSTRACT

This paper focuses on comparing the effectiveness of selected convolutional neural networks (CNNs) for face recognition. Experiments were conducted using the Labeled Faces in the Wild (LFW) dataset, testing various pre-trained CNN architectures available in MATLAB. The classification accuracy and computational efficiency of individual networks were evaluated. Results demonstrated significant performance variability among CNN architectures, with DarkNet-19 and DenseNet-201 achieving the highest accuracy. The findings confirmed that CNN accuracy is heavily influenced by network architecture, training dataset size, and selected training parameters.

Key words:
Convolutional Neural Networks; Deep Learning; Face Recognition; Security Applications

1 Martin Haváček, VŠB – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství, Lumírova 630/13, 700 30, Ostrava, martin.havacek@vsb.cz

1 INTRODUCTION

Facial recognition is a widely used biometric identification method that has gained significant attention with the advancement of deep learning techniques. The ability to recognise individuals based on facial features plays a crucial role in security applications. Recent developments in artificial intelligence and the accessibility of neural networks have made facial recognition more widespread. Deep convolutional neural networks (CNNs) have become the state-of-the-art approach due to their ability to automatically extract hierarchical features directly from image data [1]. This study aims to compare the effectiveness of several commonly available CNN architectures for face recognition. The evaluation is performed using the Labeled Faces in the Wild (LFW) dataset in a controlled experimental setup, which is widely used as a benchmark for assessing the performance of facial recognition models [2]. The performance of the models is assessed based on accuracy and computational efficiency.

2 METHODOLOGY

This chapter details the experiments conducted to study image recognition and classification using convolutional neural networks (CNNs), fundamental in contemporary deep learning frameworks [1,2]. The experimental section is structured to incrementally evaluate the effectiveness of various CNN architectures. To achieve this, the experimental part was divided into Experiment A and Experiment B. The primary aim of these experiments is to compare the performance of the selected CNNs using identical input parameters.

2.1 EXPERIMENTAL STRATEGY

The experimental part of this article was divided into two main parts, labeled Experiment A and Experiment B:

• Experiment A: This experiment conducted a baseline comparison of the available pre-trained CNNs trained on a smaller sample of a large face recognition dataset. The experiment was carried out in the MATLAB software environment. All pre-trained CNNs available in the Deep Learning Toolbox were tested, except for the NASNetLarge network due to its high computational demands.

• Experiment B: This experiment focused on comparing selected CNNs trained on a moderately sized dataset, considering the available computational resources. The models for this experiment were selected based on the results of Experiment A.

2.2 SOFTWARE AND HARDWARE

The following software and hardware resources were used to conduct the experiments:

• MATLAB: The MATLAB software, known for its efficiency in mathematical operations, simulations, and data visualization, was used to test the pre-trained algorithms. The MATLAB Online platform was also used to speed up the training process.

• Deep Learning Toolbox: This toolbox within the MATLAB environment provided the necessary functions for designing, training, and implementing deep neural networks, crucial for testing pre-trained CNN models.

• Parallel Computing Toolbox: The use of this toolbox enabled parallel computations on multiple cores simultaneously, significantly accelerating the implementation of the experimental part of the article.

• Virtual Machines: Various virtual machines with the following minimum specifications were used for training CNNs with large depth and a high number of parameters:

– RAM: 30–45 GB
– CPU: 8 cores
– GPU: 16 GB

• Hardware: Two personal computers (their specifications are provided in the original source) along with the MATLAB Online platform were crucial for the computational tasks associated with training and testing deep learning models.

2.3 TRAINING DATASET

Given limited computational resources, the Labeled Faces in the Wild (LFW) dataset [6] was selected for training the CNN models. This dataset contains more than 13,000 face images belonging to approximately 5,749 individuals and is commonly used for evaluating CNN architectures [2,3,6].

• For Experiment A, only a portion of the LFW dataset was used, specifically the categories starting with the letter A (a total of 432 categories).

• For Experiment B, the entire LFW dataset (5,749 categories) was used.

The images in the dataset were resized to 224x224 pixels before processing. The dataset is already structured into categories according to individuals. For training and validation purposes, the dataset was divided into

training and validation sets in a 70:30 ratio. This division aimed to increase the realism of the model's accuracy estimate and prevent overfitting. TheaugmentedImageDatastore function was used for data preprocessing to adjust the image sizes.

2.4 CNN SETUP (EXPERIMENT A & B)

Uniform basic training parameter settings were used for both experiments to enable relevant comparison of the results:

• Initial Learning Rate: Set to 0.001 and was not dynamically changed during training.

• Number of Epochs: 5 epochs for Experiment A, 30 epochs for Experiment B.

• Batch Size: 64 for Experiment A, 128 for Experiment B.

• Solver: The Stochastic Gradient Descent with Momentum (SGDM) optimization algorithm was used for both experiments with a momentum value of 0.9.

Other training parameters, such as L2 regularization and gradient thresholding method, were set according to default values or explicitly specified in the training options configuration. The CNN training itself was performed using the trainNetwork function in MATLAB, which took the preprocessed training data, the definition of the CNN architecture, and the training parameter settings as input. The output was a trained network and a structure containing information about the training progress.

3 RESULTS

3.1 EXPERIMENT A

Experiment A focuses on comparing different CNN architectures to assess their performance and computational efficiency. The experiment was carried out on a small dataset chosen considering the available computational resources. Furthermore, a statistical comparison of the obtained results is performed.

Comparison of Selected CNNs

CNNs were tested on a small dataset due to the high computational power required for training on a large dataset. Table 1 shows the final validation accuracy.

• The highest validation accuracies in Experiment A were achieved by DarkNet-19 (47.52%) and DarkNet-53 (46.28%).

• The lowest accuracies were exhibited by Xception (9.50%) and Inception-ResNet-v2 (9.50%).

• DenseNet-201 (35.54%) and MobileNet-v2 (27.69%) also achieved relatively good results.

Table 1 CNN Architecture Comparison Results - Experiment A

CNN Name	Final Accuracy (%)
SqueezeNet	16.12
GoogleNet	9.92
Inception-v3	18.60
DenseNet-201	35.54
MobileNet-v2	27.69
ResNet-18	27.69
ResNet-50	28.51
ResNet-101	30.58
Xception	9.50
Inception-ResNet-v2	9.50
ShuffleNet	25.21
NASNet-Mobile	11.16
DarkNet-19	47.52
DarkNet-53	46.28
EfficientNet-b0	9.92
AlexNet	27.69
VGG-16	23.14
VGG-19	28.10

Statistical Evaluation of Selected CNNs

Based on the results shown in Table 1, GoogleNet and DarkNet-19 CNNs were selected because these two pre-trained CNNs represented the worst and best results. The aim was to perform statistical tests on multiple (10) training samples.

Table 2 GoogLeNet and DarkNet-19 training statistics

Statistic	GoogLeNet	DarkNet-19
Average accuracy	11.61 %	41.16 %
Median accuracy	11.99 %	40.50 %
Standard deviation	1.65 %	1.89 %
Minimum accuracy	8.68 %	38.02 %
Maximum accuracy	14.00 %	45.04 %
Range	5.32 %	7.02 %

• GoogLeNet: Achieved the lowest accuracy of 8.68% and a highest of 14%. The standard deviation was calculated as 1.65%. The original measurement result in Table 1 was 9.92%.

• DarkNet-19: Achieved accuracies ranging from 38.02% to 45.04% in ten iterations. The standard deviation was determined to be 1.89%. In Table 1, the initial accuracy measurement was 47.52%.

The statistical comparison of GoogLeNet and DarkNet-19 (see Table 2) showed that the average accuracy differed significantly (GoogLeNet 11.61%, DarkNet-19 41.16%), but the standard deviation and range (difference between maximum and minimum accuracy) were quite similar.

Evaluation of Experiment A

Experiment A demonstrated that the tested networks differ significantly in terms of accuracy and computation time, indicating a large variance between the efficiency and performance of CNN architectures. Densely connected networks, especially DenseNet-201 and DarkNet-19, achieved good accuracy results. Repeated training of the networks with the best and one of the worst accuracy results showed similar standard deviations and ranges, suggesting that the variability of the results was not dependent on the achieved accuracy.

3.2 EXPERIMENT B

Based on the results of Experiment A, a total of five pre-trained CNNs representing below-average, average, and above-average results were selected: AlexNet, DarkNet-19, GoogLeNet, ShuffleNet, and SqueezeNet. The comparison was performed on the entire dataset and with a larger number of epochs.

• AlexNet: Achieved a final accuracy of 31.92% and a loss of 5.9. Overfitting was observed around the 15th epoch.

• DarkNet-19: Achieved a final accuracy of 38% and a loss of 5.02. Significant overfitting was observed around the 21st epoch, reaching 100% accuracy on the training data.

• GoogLeNet: Achieved a final accuracy of 30.38% and a loss of 5.74. Overfitting was observed around the 21st epoch.

• ShuffleNet: Achieved a final accuracy of 31.92% and a loss of 5.24. No significant overfitting was observed for this network.

• SqueezeNet: Achieved a final accuracy of 18.78% and a loss of 8.4. Overfitting was observed around the 14th epoch.

Evaluation of Experiment B

Table 3 summarizes the results of Experiment B. DarkNet-19 achieved the best validation accuracy and the lowest loss value but exhibited overfitting. GoogLeNet also achieved a relatively good result. AlexNet and ShuffleNet achieved similar validation accuracies, but ShuffleNet showed a better validation loss result and did not exhibit overfitting. SqueezeNet achieved the worst validation accuracy and loss.

Table 3 Validation Results of Experiment B Comparison

CNN Name	Final ACC (%)	Final Loss	Overfitting
SqueezeNet	18.78	8.4	Yes
GoogLeNet	30.82	5.74	Yes
ShuffleNet	31.92	5.24	No
DarkNet-19	38.00	5.02	Yes
AlexNet	31.92	5.9	Yes

3.3 COMPARISON OF THE RESULTS OF EXPERIMENTS A AND B

Table 4 compares the results of Experiment A and Experiment B.

• SqueezeNet achieved similar final validation accuracies in both experiments.

• GoogLeNet, AlexNet, and ShuffleNet achieved significantly better final validation accuracies in Experiment B.

• DarkNet-19 was the only network that achieved worse results in Experiment B than in Experiment A.

The results of the experimental part indicate that the performance of different CNN architectures varies significantly for the task of face recognition and is influenced by both the network architecture and the training parameters and size of the training dataset.

Table 4 Comparison Validation Accuracy from Experiment A and B

CNN Name	Final ACC (Experiment A) (%)	Final ACC (Experiment B) (%)
SqueezeNet	16.12	**18.78**
GoogLeNet	9.92	30.82
Inception-v3	18.60	---
DenseNet-201	35.54	---
MobileNet-v2	27.69	---
ResNet-18	27.69	---
ResNet-50	28.51	---
ResNet-101	30.58	---
Xception	**9.50**	---
Inception-ResNet-v2	**9.50**	---
ShuffleNet	25.21	31.92
NASNet-Mobile	11.16	---
DarkNet-19	**47.52**	**38.00**
DarkNet-53	46.28	---
EfficientNet-b0	9.92	---
AlexNet	27.69	31.92
VGG-16	23.14	---
VGG-19	28.10	---

4 DISCUSSION

The results align with previous findings that demonstrate the varying efficiency and accuracy of CNN architectures on face recognition tasks [4,5]. Deep CNNs typically achieve high accuracy but demand extensive computational resources, whereas lighter architectures can provide balanced accuracy and efficiency [5]. This trade-off should inform the selection of CNN models for practical security applications.

REFERENCES

[1] GUO, G., ZHANG, N. 2019. A survey on deep learning based face recognition. In: Computer Vision and Image Understanding. Vol. 189, 2019, pp. 102805.

[2] WANG, M., DENG, W. 2021. Deep face recognition: A survey. In: Neurocomputing. Vol. 429, 2021, pp. 215–244.

[3] GWYN, T., ROY, K., ATAY, M. 2021. Face Recognition Using Popular Deep Net Architectures: A Brief Comparative Study. In: Future Internet. Vol. 13, No. 7, 2021, pp. 164.

[4] NEMAVHOLA, A., CHIBAYA, C., VIRIRI, S. 2025. A Systematic Review of CNN Architectures, Databases, Performance Metrics, and Applications in Face Recognition. In: Information. Vol. 16, No. 2, 2025, pp. 107.

[5] RODRIGO, M., CUEVAS, C., GARCÍA, N. 2024. Comprehensive comparison between vision transformers and convolutional neural networks for face recognition tasks. In: Scientific Reports. Vol. 14, 2024, pp. 21392.

[6] HUANG, G. B., RAMESH, M., BERG, T., LEARNED-MILLER, E. 2007. Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments. University of Massachusetts, Amherst, Technical Report 07-49.

IMPLEMENTÁCIA POŽIARNEHO MODELOVANIA DO PRAXE

Dorota Hodúlová[1], Stanislava Gašpercová[2]

ABSTRAKT

Určovanie odstupových vzdialeností medzi stavbami je v dnešnej dobe čoraz dôležitejšie, nakoľko rastúci počet nových budov zvyšuje riziko prenosu požiaru. Tento článok sa zameriava na využitie požiarnych modelov, ako je FDS na simuláciu požiarov a šírenia tepla v uzatvorených priestoroch s cieľom implementácie požiarnych modelov do praxe. Implementácia požiarnych modelov vyžaduje analýzu citlivosti na dosiahnutie optimálnych výsledkov, ktoré prispievajú k presnému stanoveniu a relevantným výsledkom odstupových vzdialeností, čo je cieľom príspevku.

Kľúčové slová:
Protipožiarna bezpečnosť stavieb, Odstupové vzdialenosti, Požiarne modely, Fire Dynamics Simulator, Vzdelávanie.

ABSTRACT

Determining stand-off distances between buildings is increasingly important nowadays, as the growing number of new buildings increases the risk of fire transmission. This paper focuses on the use of fire models such as FDS to simulate fires and heat spread in confined spaces with the aim of implementing fire models into practice. The implementation of fire models requires sensitivity analysis to achieve optimal results that contribute to accurate determination and relevant stand-off distance results, which is the objective of the paper.

Key words:
Fire safety solution for buildings, Stand-off distances, Fire models, Fire Dynamics Simulator, Education.

1 Ing. Dorota Hodúlová, Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, ul. 1. mája 32, Žilina 010 01, dorota.hodulova@uniza.sk, 041 513 6769
2 doc. Ing. Bc. Stanislava Gašpercová, PhD., Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, ul. 1. mája 32, Žilina 010 01, stanislava.gaspercova@uniza.sk, 041 513 6796

1 ÚVOD

V súčasnosti dochádza k výraznému nárastu výstavby nových stavieb a k rekonštrukciám starých stavieb čo spôsobuje znižovanie dostupnosti stavebných pozemkov, na ktorých je možné umiestniť stavby bez riešenia problematiky prenosu požiaru medzi stavbami. Na účinnú prevenciu prenosu požiaru je potrebné poznať nielen vzdialenosť medzi stavbami, ale aj správanie sa požiaru. Pomocou požiarne nebezpečného priestoru sa určuje potrebná vzdialenosť medzi stavbami na zabránenie prenosu požiaru. Požiarne modely sú nástroje simulácie požiarov, najmä v uzatvorených priestoroch, vďaka ktorým je možné predpovedať jeho správanie pri ovplyvnení rôznych faktorov. Vďaka takýmto simuláciám je možné minimalizovať škody a chrániť zdravie a životy ľudí. Implementácia požiarnych modelov do praxe je v podmienkach Slovenskej republiky neznáma, pričom vo svete je aplikácia požiarnych modelov bežnou súčasťou riešenia protipožiarnej bezpečnosti stavieb.

Cieľom príspevku je poukázanie na možnosť využívania požiarnych modelov, ako je FDS, v rámci riešenia protipožiarnej bezpečnosti stavieb na Slovensku so zameraním na odstupové vzdialenosti. Súčasťou cieľa je spracovanie citlivostnej analýzy, vytvorenie všeobecného modelu riešenia odstupových vzdialeností a jeho overenie.

2 POŽIARNE NEBEZPEČNÝ PRIESTOR

Požiarne nebezpečný priestor [1] je priestor, ktorý sa vytvára okolo horiaceho požiarneho úseku alebo objektu, v ktorom je nebezpečie prenosu požiaru sálaním tepla, alebo padajúcimi časťami konštrukcie, ktoré by mohli šíriť požiar na iný objekt alebo iný požiarny úsek tej istej stavby. Požiarne nebezpečný priestor sa v stavbe určuje na základe požiarneho rizika. Požiarne riziko je definované ako pravdepodobná intenzita požiaru v požiarnom úseku alebo jeho časti. Požiarne riziko sa vyjadruje ekvivaletným časom trvania požiaru (min) pre výrobné stavby, výpočtovým požiarnym zaťažením ($kg.m^{-2}$) pre nevýrobné stavby, indexom skladovaných materiálov a indexom ekonomického rizika pre sklady v jednopodlažnej stavbe [1, 2]. K analýze problematiky riešenia odstupových vzdialeností sa na Slovensku používajú všeobecne platné právne predpisy a technické normy, ktoré súvisia s problematikou protipožiarnej bezpečnosti stavieb vo všeobecnosti. Základnými právnymi predpismi pri vypracovaní projektovej dokumentácie protipožiarnej bezpečnosti stavieb na Slovensku sú [3 – 6]:

- *Zákon NR SR č. 314/2001 Z. z. o ochrane pred požiarmi v znení neskorších predpisov*.
- *Vyhláška MV SR č. 121/2002 Z. z. o požiarnej prevencii v znení neskorších predpisov.*
- *Zákon NR SR č. 25/2025 Z. z. Stavebný zákon.*

- *Vyhláška MV SR č. 94/2004 Z. z. ktorou sa ustanovujú technické požiadavky na protipožiarnu bezpečnosť pri výstavbe a pri užívaní stavieb v znení neskorších predpisov.*

Protipožiarna bezpečnosť stavieb sa na Slovensku rieši Slovenskými technickými normami (ďalej len STN), ktoré nie sú právne záväzné, ale ich znenie je povinné ak sa na STN odkazuje niektorý vykonávajúci predpis [1,2, 7 – 12] :

- STN 92 0201 – 1: Protipožiarna bezpečnosť stavieb – Požiarne riziko, veľkosť požiarneho úseku.
- STN 92 0201 – 2: Protipožiarna bezpečnosť stavieb – Stavebné konštrukcie.
- STN 92 0201 – 3: Protipožiarna bezpečnosť stavieb – Únikové cesty a evakuácia.
- STN 92 0201 – 4: Protipožiarna bezpečnosť stavieb – Odstupové vzdialenosti.
- STN 92 0400: Zásobovanie vodou na hasenie požiarov.
- STN 92 0202 – 1: Vybavenie stavieb hasiacimi prístrojmi.
- STN 92 0241: Obsadenie stavieb osobami.

3 RIEŠENIE ODSTUPOVÝCH VZDIALENOSTÍ POŽIARNYMI MODELMI

Požiarne modely predstavujú simulácie požiarov, ktoré sa môžu využívať pri riešení protipožiarnej bezpečnosti stavieb. Existuje nespočetné množstvo požiarnych modelov. Každý požiarny model má za úlohu najmä nasimulovať požiar a prenos dymu, pričom ale každý kladie dôraz na iné parametre ich vývoja. Každý model pracuje iným spôsobom a s inou presnosťou. Príspevok sa zaoberá požiarnym modelom FDS, nakoľko tento model je presný a voľne dostupný [13, 14].

Základom modelovania priestoru v programe FDS je vytvorenie výpočtovej siete, ktorá sa skladá z výpočtových buniek so stanovenými rozmermi. V jednom modeli môže byť viacero sietí, pričom bunky, ktoré sa dotýkajú, by mali mať rovnaké pomery. Pre posudzovanie odstupových vzdialeností postačuje jedna výpočtová sieť, ktorej veľkosť závisí od počtu a veľkosti otvorov a ich vzdialenosti. Bunky by mali mať rovnaké rozmery vo všetkých smeroch pre optimalizáciu výpočtov, čo je dôležité pre presnosť simulácie tepla, požiaru a splodín horenia v celej sieti [14].

Steny výpočtovej siete sú definované ako inertné plochy, ktoré nepodliehajú chemickým reakciám, čo je žiaduce pri posudzovaní odstupových vzdialeností od úplne požiarne otvorených plôch stavby. Všetky steny okrem jednej by mali byť otvorené, simulujúce vonkajší priestor. Jedna stena zostáva inertná a simuluje stenu s úplne požiarne otvorenými plochami. Ak sa posudzuje aj čiastočne požiarne otvorená plocha, je možné upraviť povrch tejto steny.

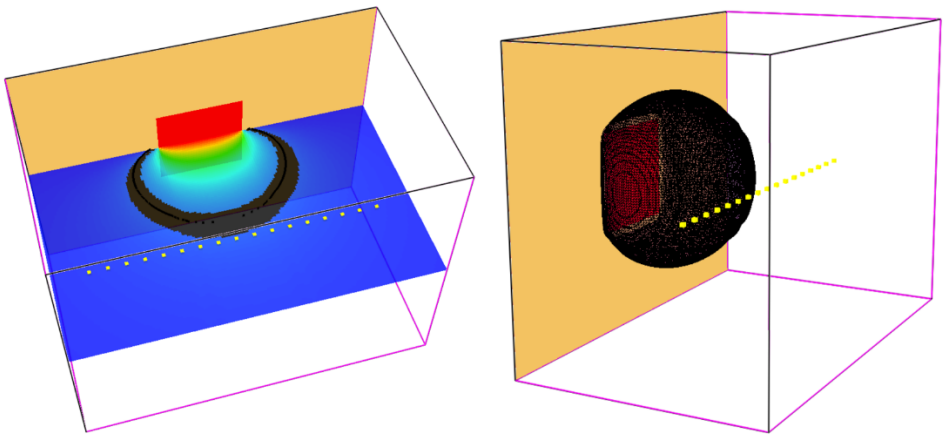
Pre posudzovanie odstupových vzdialeností od úplne požiarne otvorených plôch sa do inertnej steny umiestnia sálavé plochy, ktoré simulujú únik tepla cez otvory. Počet a rozmery týchto plôch závisia od skutočných otvorov v konštrukcii a teplota alebo plošná hustota tepelného toku sa nastavuje podľa požiadaviek. Pre presnosť sa používajú konštantné hodnoty týchto veličín počas požiaru. Hodnoty sálavej plochy sa určujú na základe normovej teplotnej krivky (1) a (2), ktorá zohľadňuje ekvivalentný čas požiaru alebo požiarne zaťaženie stavby [15].

$$T_N = 20 + 345 \log (8t + 1) \quad (1)$$

$$q = (T_N + 273)^4 \cdot 5{,}67 \cdot 10^{-11} \quad (2)$$

Odstupová vzdialenosť sa určuje meraním vybranej veličiny pomocou meracích zariadení. FDS ponúka 11 rôznych zariadení na zaznamenávanie veličín súvisiacich s tepelnou expozíciou povrchov, ktoré sa líšia v meraní prenosu energie a umiestnení buď na pevnej ploche, alebo vo vzduchu. Tieto zariadenia sú podrobne popísané v *Fire Dynamics Simulator User's Guide, kapitola* 22.10.12 *Heat Flux* [14]. Pre určenie odstupových vzdialeností je ideálne použiť zariadenie *Gauge Heat Flux Gas*, ktoré zaznamenáva sálavé aj prúdiace teplo a môže byť umiestnené vo voľnom priestore.

Zariadenia sa môžu umiestniť v ľubovoľnom počte, v závislosti od veľkosti požiarne otvorených plôch a vzdialenosti od sálavej plochy. Odhad vzdialenosti a vplyv iných parametrov na výsledky meraní sú predmetom citlivostnej analýzy. Na zaznamenávanie intenzity tepla vyžarujúceho zo sálavej plochy je potrebné definovať *Slice File* Parameter vo vstupnom súbore. Tento parameter umožňuje zaznamenávanie veličín plynnej fázy v strede sálavej plochy v horizontálnom alebo vertikálnom smere. Odstupová vzdialenosť sa odčítava na základe hraničnej hodnoty 18,5 $kW.m^{-2}$, ktorá sa vykreslí v 2D v nasimulovanom priestore. V FDS je tiež možné vytvoriť trojrozmerné veličiny plynnej fázy a zobraziť odstupovú vzdialenosť v 3D pomocou príkazu *Isosurface Parameter*. Príklad vykreslenia v 2D a 3D je zobrazený na Obrázku 1.



Obrázok 1 Vykreslenie odstupovej vzdialenosti v 2D a 3D

Aby bolo možné v praxi využiť požiarne modely pri určovaní odstupových vzdialeností od stavieb, je potrebné vykonať množstvo simulácií, ktoré postupne preskúmajú vplyv jednotlivých vstupných parametrov na celkový výpočtový čas, presnosť odčítania a vykreslenia odstupových vzdialeností, ako aj na veľkosť odstupovej vzdialenosti. Tento proces sa nazýva citlivostná analýza alebo validácia. Podľa informácií z *Fire Dynamics Simulator User's Guide* a skúseností s programom FDS majú na výpočtový čas a veľkosť odstupovej vzdialenosti najväčší vplyv nasledujúce parametre [14]:

- *Veľkosť výpočtových buniek* vo výpočtovej mriežke.
- *Dĺžka cesty (Path Length)* [m] – tento parameter je dôležitý pri určovaní a zachytávaní hodnôt prenosu radiácie v priestore požiaru. V rámci výpočtu tepelného toku tento parameter udáva vzdialenosť medzi požiarom a meracím zariadením (cieľom).
- *Počet priestorových radiačných uhlov (Number Radiation Angles)* – tento parameter zlepšuje priestorovú a časovú presnosť diskrétnej rovnice prenosu žiarenia, čím ovplyvňuje vizualizáciu kritických hodnôt pri určovaní odstupových vzdialeností. Čím menší je počet priestorových radiačných uhlov, tým má vizualizácia hviezdicovitejší tvar a naopak, čím je počet väčší, tým je vizualizácia kritickej hodnoty hladšia a približuje sa k tvaru oválu.
- *Prírastok časového kroku (Time Step Increment)* a *Prírastok uhlov (Angle Increment)* – tieto parametre ovplyvňujú frekvenciu výstupov zaznamenávaného žiarenia. Prednastavená hodnota prírastku časového kroku je 3 a prírastku uhlov 5. V takomto prípade, dôjde každých 15 časových krokov k aktualizácii rovnice prenosu žiarenia a teda k zaznamenaniu hodnôt. Ak hodnoty oboch parametrov budú 1, tak k zaznamenaniu hodnôt dôjde každý 1 časový krok.
- *Relatívna vlhkosť vzduchu (Humidity)* – tento parameter nadobúda hodnoty v rozmedzí 0-100, pričom prednastavená hodnota je 40 %.

4 IMPLEMENTÁCIA POŽIARNYCH MODELOV DO PRAXE

V rámci citlivostnej analýzy bolo vykonaných celkovo viac ako 180 simulácií so zameraním na vplyv jednotlivých parametrov na celkový výpočtový čas simulácií a výslednú hodnotu odstupovej vzdialenosti.

Zistilo sa, že parameter *Dĺžka cesty* nemá vplyv na celkový výpočtový čas simulácií, keďže všetky simulácie trvali 250 s. Parameter *Relatívna vlhkosť vzduchu* mal vplyv na výpočtový čas simulácií a to v rozsahu + 27 % výpočtového času. Simulácie, pri ktorých bola vlhkosť 0 %, trvali 250 s a pri 100 % 345 s. Parametre *Počet priestorových radiačných uhlov*, *Prírastok časového kroku* a *Prírastok uhla* mali významný vplyv, pričom došlo k zvýšeniu výpočtového času až o + 600 %. Najväčší vplyv mal parameter *Veľkosť výpočtových buniek*, kedy sa skúmali štyri veľkosti výpočtovej bunky 10 mm, 25 mm, 50 mm a 75 mm. V prípade veľkosti výpočtovej siete 75 mm bol čas

simulácie len niekoľko sekúnd, zatiaľ čo v prípade veľkosti výpočtovej siete 10 mm to bolo rádovo niekoľko dní.

Vplyv vybraných parametrov na veľkosť odstupových vzdialeností sa ako prvé skúmal v súvislosti s parametrami *Prírastok časového kroku* a *Prírastok uhla*. Tieto parametre neovplyvňujú výslednú hodnotu odstupovej vzdialenosti, pretože hodnota odstupovej vzdialenosti podľa normatívneho prístupu aj podľa simulácií bola 1,2 m. Aj napriek tomu, že uvedené parametre nemali vplyv na výslednú hodnotu odstupovej vzdialenosti sa odporúča , aby sa hodnoty parametrov menili nasledovne, *Time Step Increment 1* a *Angle Increment 1*, aby sa žiarenie zaznamenávalo každý jeden časový krok.

Pre parameter *Relatívna vlhkosť vzduchu* sa zistilo, že hodnota odstupovej vzdialenosti podľa normatívneho prístupu je 1,2 m. Pre hodnoty vlhkosti 40 % a 50 % sú hodnoty odstupovej vzdialenosti podľa FDS tiež 1,2 m. Pri nižších hodnotách *Relatívnej vlhkosti vzduchu* sa vzdialenosť odstupu zvýšila až o 11 % a pri vyšších hodnotách *Relatívnej vlhkosti vzduchu* sa vzdialenosť odstupu znížila až o 9 %. Z uvedených výsledkov vyplýva, že uvedený parameter ovplyvňuje výsledné odstupové vzdialenosti určené programom FDS. V rámci určovania odstupových vzdialeností programom FDS a v rámci bezpečnosti by bolo najvhodnejšie použiť pri simuláciách hodnotu relatívnej vlhkosti 0 %. Najvhodnejšie je vždy pracovať s predpokladanou skutočnou hodnotou parametru prípadoch, keď sa tento parameter nedá presne určiť, odporúča sa použiť predvolenú hodnotu 40 %.

Na základe posúdenia vplyvu parametrov *Dĺžka cesty* a *Počet priestorových radiačných uhlov* sa dospelo k záveru, že parameter *Počet priestorových radiačných uhlov* nemá žiadny vplyv na výslednú hodnotu odstupovej vzdialenosti pre veľkosť výpočtovej bunky 25 mm. Na základe už získaných poznatkov o fungovaní programu však možno tvrdiť, že tento parameter môže ovplyvniť vykresľovanie odstupových vzdialeností v rámci tvaru výslednej odstupovej vzdialenosti, t. j. či má približne tvar elipsy alebo skôr hviezdy. V prípade tvaru hviezdy by výstupky útvaru mohli spôsobiť rozdiely v odstupových vzdialenostiach rádovo od 0 cm do 5 cm. Parameter *Dĺžka cesty* má preukázateľný vplyv na celkovú hodnotu výslednej odstupovej vzdialenosti. Čím nižšia je hodnota *Dĺžky cesty* v FDS, tým nižšia je výsledná hodnota odstupovej vzdialenosti v porovnaní s hodnotou pozorovanou pri väčšej hodnote daného parametru. Maximálny pozorovaný rozdiel je 6 %, čo predstavuje 0,1 m.

Parameter *Veľkosť výpočtovej bunky* má mierny vplyv na veľkosť výsledných odstupových vzdialeností. Veľkosť rozdielov sa pohybovala od 0 cm do 7 cm, čo predstavuje rozdiel v simuláciách, ktorý sa určil v rozmedzí od 0 % do 4 %. Pri zistených výsledkoch nemožno povedať, že zmenšenie alebo zväčšenie výpočtovej siete malo konkrétny vplyv na výslednú odstupovú vzdialenosť, pretože nebol pozorovaný žiadny trend, ktorý by sa opakoval medzi simuláciami s rôznymi veľkosťami sálavej plochy. Pokiaľ však ide o uvedené

výsledky, možno tvrdiť, že rozdiel vo výsledkoch odstupových vzdialeností môže byť spôsobený veľkosťou výpočtových buniek v zmysle možnosti odčítania odstupovej vzdialenosti len v intervaloch veľkosti výpočtových buniek.

Posledným skúmaným parametrom bol *Počet meracích zariadení*. Podľa výsledkov získaných simuláciami sa dospelo k záveru, že parameter neovplyvňuje výsledné hodnoty odstupových vzdialenostiach pri uvedených parametroch simulácií. Rozdiely vo výsledných hodnotách by sa mohli vyskytnúť , ak by sa v simuláciách použili len 2 - 3 meracie zariadenia alebo ak by sa výpočtová sieť zmenšila na veľkosť výpočtovej bunky napríklad 10 mm. V takomto prípade by mohlo dôjsť k miernym zmenám v určení výsledných odstupových vzdialeností, ale tie by v prípade zmenšenia výpočtovej bunky spočívali najmä v možnosti odčítania výsledkov v intervale veľkosti výpočtových buniek.

Všetky výsledky získané z citlivostnej analýzy bolo potrebné spracovať a vytvoriť všeobecný model riešenia odstupových vzdialeností budov pomocou požiarnych modelov. Vytvorený model bol použitý na overenie hodnôt odstupových vzdialeností pre jednotlivé otvory úplne požiarne otvorených plôch podľa STN 92 0201 – 4 [1], čím je možné potvrdiť alebo vyvrátiť správne nastavenie požiarneho modelu a možnosť jeho implementácie v praxi v podmienkach Slovenskej republiky. Celkovo bolo v rámci overovania hodnôt odstupových vzdialeností vytvorených až 540 simulácií. Vzhľadom na veľké množstvo údajov sú v Tabuľke 1 uvedené len niektoré vybrané hodnoty. Vzťah prepočtu hodnoty požiarneho rizika na teplotu sálavej plochy je uvedený v kapitole 3 Riešenie odstupových vzdialeností požiarnymi modelmi - rovnica 1.

Tabuľka 1 Porovnanie hodnôt odstupových vzdialeností normatívneho prístupu a FDS

Dĺžka otvoru [m]	**Výška otvoru [m]**	**Požiarne riziko (p_v [kg,m^{-2}] or t_e [min])**							
		10		**40**		**80**		**180**	
		678 °C		**885 °C**		**988°C**		**1 110 °C**	
		STN	**FDS**	**STN**	**FDS**	**STN**	**FDS**	**STN**	**FDS**
0,5	0,5	0,30	0,35	0,60	0,60	0,70	0,75	0,90	0,95
		14%		0%		7%		5%	
1,0	1,0	0,70	0,70	1,20	1,20	1,50	1,60	1,80	1,85
		0%		0%		6%		3%	
2,0	2,5	1,50	1,60	2,70	2,65	3,50	3,45	4,00	3,95
		6%		-2%		-1%		-1%	
3,0	2,5	1,90	1,85	3,30	3,25	4,30	4,15	4,90	4,70
		-3%		-2%		-4%		-4%	
3,5	2,0	1,80	1,85	3,50	3,50	4,60	4,45	5,30	5,05
		5%		0%		-3%		-5%	
4,0	3,0	2,50	2,55	4,40	4,70	5,40	5,20	6,60	6,10
		2%		-2%		-4%		-8%	

Výsledky získané zo simulácií ukazujú, že program FDS je vhodný na riešenie odstupových vzdialeností od úplne požiarne otvorených plôch, len ak sú správne nastavené všetky vstupné parametre. Najväčšie rozdiely, pri ktorých hodnota FDS vyšla väčšia ako hodnota STN, boli 0,25 m a 0,3 m. Tieto rozdiely boli zaznamenané najmä pri väčších otvoroch predstavujúcich úplne požiarne otvorenú plochu, t.j. pri otvoroch s dĺžkou 4,0 m a 4,5 m. V percentuálnom vyjadrení boli tieto rozdiely v rozmedzí 8 % až 19 %.

V mnohých prípadoch sa pozoroval aj rozdiel medzi hodnotami, kedy hodnota výslednej odstupovej vzdialenosti od FDS vyšla menšia ako v norme. V tomto prípade bola percentuálna hodnota rozdielu zaznamenaná ako záporná. Takéto výstupy sú viditeľné najmä pri otvoroch s dĺžkou väčšou ako 1,5 m. Rozdiely sa v tomto prípade pohybovali od 0,05 m do 0,5 m, čo predstavovalo približne 1 až 8 % rozdielu.

5 ZÁVER

V oblasti požiarnej bezpečnosti stavieb je dôležité zohľadniť všetky faktory, ktoré ovplyvňujú samotný požiar, ako napríklad účel využitia stavby, jej výška alebo vzdialenosť od iných budov. S rastúcou hustotou zástavby rastie potreba riešenia prenosu požiarov medzi stavbami a určovania odstupových vzdialeností medzi budovami, aby sa minimalizovalo riziko šírenia požiaru. V rámci riešenia uvedenej problematiky je možné implementovať požiarne modely, ktoré simulujú požiare v rôznych podmienkach, a umožňujú tak ich implementáciu pri návrhu vybraných častí stavieb, ako sú aj odstupové vzdialenosti.

Požiarne modely, ako napríklad FDS, poskytuje účinnú analýzu požiarov v uzavretých priestoroch. Tento model umožňuje nielen simuláciu šírenia požiaru, ale aj meranie rôznych premenných súvisiacich s tepelnou expozíciou, čo je nevyhnutné pri určovaní odstupových vzdialeností medzi budovami. Na základe výpočtov a simulácií je možné lepšie pochopiť vplyv rôznych parametrov na simuláciu odstupových vzdialeností. Hoci je implementácia týchto modelov v praxi ešte len vo fáze výskumu, ich potenciál v oblasti riešenia protipožiarnej bezpečnosti stavieb je veľký, čo potvrdila aj citlivostná analýza a porovnanie výsledných hodnôt odstupových vzdialeností normatívneho prístupu a simulácií.

POĎAKOVANIE

Tento článok bol podporený projektom 041ŽU-4/2023, Vzdelávací a výcvikový modul rozširujúci znalosti, zručnosti a kompetencie študentov programu záchranné služby

LITERATÚRA

[1] STN 92 0201 - 4: 2000, *Požiarna bezpečnosť stavieb – Odstupové vzdialenosti.*

[2] STN 92 0201 – 1: 2000, *Požiarna bezpečnosť stavieb – Požiarne riziko, veľkosť požiarneho úseku.*

[3] *Zákon NR SR č. 314/2001 Z. z. o ochrane pred požiarmi v znení neskorších predpisov*

[4] *Vyhláška MV SR č. 121/2002 Z. z. o požiarnej prevencii v znení neskorších predpisov.*

[5] *Zákon NR SR č. 25/2025 Z. z. Stavebný zákon v znení neskorších predpisov.*

[6] *Vyhláška MV SR č. 94/2004 Z. z. ktorou sa ustanovujú technické požiadavky na protipožiarnu bezpečnosť pri výstavbe a pri užívaní stavieb v znení neskorších predpisov.*

[7] STN 92 0201 – 2: 2017, *Požiarna bezpečnosť stavieb – Stavebné konštrukcie.*

[8] STN 92 0201 - 3: 2000, *Požiarna bezpečnosť stavieb – Únikové cesty a evakuácia osôb.*

[9] STN 92 0400: 2005, *Požiarna bezpečnosť stavieb – Zásobovanie vodou na hasenie požiarov.*

[10] STN 92 0202 - 1: 1999, *Požiarna bezpečnosť stavieb – Vybavenie stavieb hasiacimi prístrojmi.*

[11] STN 92 0241: 2012, *Požiarna bezpečnosť stavieb – Obsadenie stavieb osobami.*

[12] STN EN 1991-1-2:2007, *Zaťaženie konštrukcií, Časť 1-2: Všeobecné zaťaženia – Zaťaženia konštrukcií namáhaných požiarom.*

[13] BEYLER, C.L. a kol. 2008. *Introduction to Fire Modeling*. Zdroj: COTE, A. a LINVILLE, J. 2006. *Fire protection handbook*. National Fire Protection Association – NFPA, ISBN-13: 978-0877657583, ISBN-10: 0877657580.

[14] MCGRATTAN, K. a kol. 2013. *Fire Dynamics Simulator – User´s Guide* [online]. NIST – National Institute of Standards and Technology [cit. 2023-07-01]. Dostupné na internete: <https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=913619>.

[15] ISO 834-11:2014, *Fire resistance tests*.

SITUATIONAL PREVENTION AS A TOOL FOR THE PROTECTION OF SOFT TARGETS WITH A FOCUS ON SCHOOLS AND SCHOOL FACILITIES

Samuel Hubočan[1], Viktor Šoltés[2], Veronika Adamová[3]

ABSTRACT

In Slovakia, as in other countries, there has been and still continues to be an important debate about the protection of soft targets, i.e. places that are potentially vulnerable to terrorist or violent attacks. Even though Slovakia is not a significant target and space for such attacks, it is possible, especially at present, to identify several cases and incidents that increase the pressure to improve the security measures of objects in the domestic environment. One example is schools, school premises, and universities, which are significantly vulnerable soft targets. In the present article, the authors seek to bring the issue of situational prevention to school settings and to increase public awareness of the security risks of attacks on such facilities.

Key words:
Soft target, school, prevention, situational prevention, crime

1 INTRODUCTION

The issue of soft target protection remains a highly relevant topic, not only abroad but also in the domestic environment, as evidenced by several significant incidents and attacks. The most notable ones include:

- **Shooting on Zámocká Street in Bratislava (October 2022) -** This incident is one of the most serious recent attacks on a soft target in Slovakia. A young man shot two people (men) and injured a woman in front of an establishment on Zámocká Street in Bratislava, frequented mainly by the LGBTI+ community. This attack was classified as a terrorist act motivated by hatred towards the LGBTI+ community. The perpetrator spread hate speech on social media and was inspired by extremist ideologies. This case highlighted the vulnerability of public spaces and the growing problem of radicalization through the internet [1].

1 Ing. Samuel Hubočan, Univerzitná 8215/1, 010 26 Žilina, 0911 974 650, samuel.hubocan@uniza.sk
2 doc. Ing. Viktor Šoltés, PhD., Univerzitná 8215/1, 010 26 Žilina, 041 513 6656, viktor.soltes@uniza.sk
3 Ing. Veronika Adamová, PhD., Univerzitná 8215/1, 010 26 Žilina, 041 513 6666, veronika.adamova@uniza.sk

- **Attack at the Spojená škola in Vrútky (Jun 2020)** – This tragic incident occurred at the Spojená škola in Vrútky, highlighting the need for greater protection of soft targets, especially schools. In this case, a 22-year-old attacker armed with a knife entered school premises and assaulted staff and students. The attack resulted in one fatality (the deputy director died on the spot while attempting to stop the attacker) and several serious injuries (two students and a teacher suffered severe injuries) [2].
- **Shooting in Devínska Nová Ves (August 2010)** – This incident took place in the Bratislava district of Devínska Nová Ves, where a perpetrator armed with an automatic weapon killed 8 people (including the shooter himself) and injured 15 others. Although this attack was not considered a terrorist act, it was a serious assault on residents in their homes and public spaces, demonstrating the vulnerability of civilian targets [3].
- **Cyber Attacks on Public Institutions** – Slovakia, like other countries, faces a growing threat of cyberattacks targeting soft targets, including hospitals, schools, and government institutions. An example is the 2020 cyberattack on the nearby University Hospital in Brno. This attack led to the interruption of several operations and procedures, simultaneously highlighting the vulnerability of healthcare facilities [4]. An example from the Slovak Republic can be a ransomware attack on the National Land Register. This led to a malfunction of a significant part of public administration portals [5].
- **Bomb threats** - Various parts of Slovakia have experienced several cases of reported bomb threats in shopping centres, schools [6, 7], and other public places, both in the past and present. All of these were false alarms and spreading of "alarming news", but these incidents caused panic and showed how easily soft targets can be affected by these types of threats.
- **Knife Attack at the School in Spišská Stará Ves** – A student attacked teachers and other students with a knife. The result was the death of a teacher and a student, with 3 other patients hospitalized. The attacker was known to have tendencies towards aggression. Despite this information, insufficient security measures were taken, resulting in the attack [8].

The shooting at the Faculty of Arts of Charles University, in neighbouring Czech Republic, is another relevant case. The attack took place on December 21, 2023, in Prague, in the faculty building on Jan Palach Square. The number of victims was 14, with 24 people injured [9]. It is the most tragic shooting in the history of the Czech Republic [10].

Based on these and other real cases and events, there is a significant and justified need for protecting soft targets and minimizing the risks of attacks. In the presented article, the first chapter will describe the terminology of basic concepts, smoothly transitioning to the issue of schools and educational facilities as one of the significant and vulnerable elements of soft targets. The second

chapter of the article will outline a method of applying situational prevention in school facilities.

The aim of this paper is to assess selected situational crime prevention measures implemented in schools. The measures are based on standard STN P CEN/TS 14383-6. The aim of the assessment is to make an indicative assessment of security in the selected objects regarding the practical benefits for the schools involved.

1.1 SOFT TARGET

The term "soft target" was already used in the introduction of the article. Several authors have addressed the issue of soft targets and their definition, e.g., in publications [11, 12, 13, 14]. Authors in publication [11] define a soft target as places or situations that may be potentially vulnerable to violent attacks but are not considered part of critical infrastructure. These places may include public gatherings, cultural or sporting events, spaces where many people gather, with a low level of security. The author in publication [12] defines soft targets as civilian objects and spaces where large numbers of people gather, such as national monuments, hospitals, schools, sports halls, hotels, cultural centres, theatres, cinemas, cafes and restaurants, workplaces, nightclubs, shopping centres, and transportation networks like subways, trains, or buses. These places are less protected and vulnerable to attacks. Areas in the immediate vicinity of protected objects, such as airport halls, are also considered soft targets. According to the mentioned publications, an attack on soft targets can have serious consequences for national security and undermine confidence in the government's ability to protect the population. Tourist, shopping, and recreational centres are particularly vulnerable, especially when chemical or biological weapons are used. These facilities do not primarily focus on security, often due to lack of funds for special security measures. Therefore, they are often designated as weapon-free zones, where the only resistance to an attacker can be posed by unarmed guards. This lack of protection makes schools, churches, hospitals, and shopping centres easily accessible targets for terrorists or other attackers.

Based on the studied literature, the definition of soft targets can be generalized as follows. Soft targets represent places and spaces (objects) where many human subjects are concentrated and accumulated, while these objects are protected to a minimal, insufficient, or no extent against terrorist attacks or other violent criminal activities.

Soft targets in terms of their duration can be categorizes as follows (Figure 1)

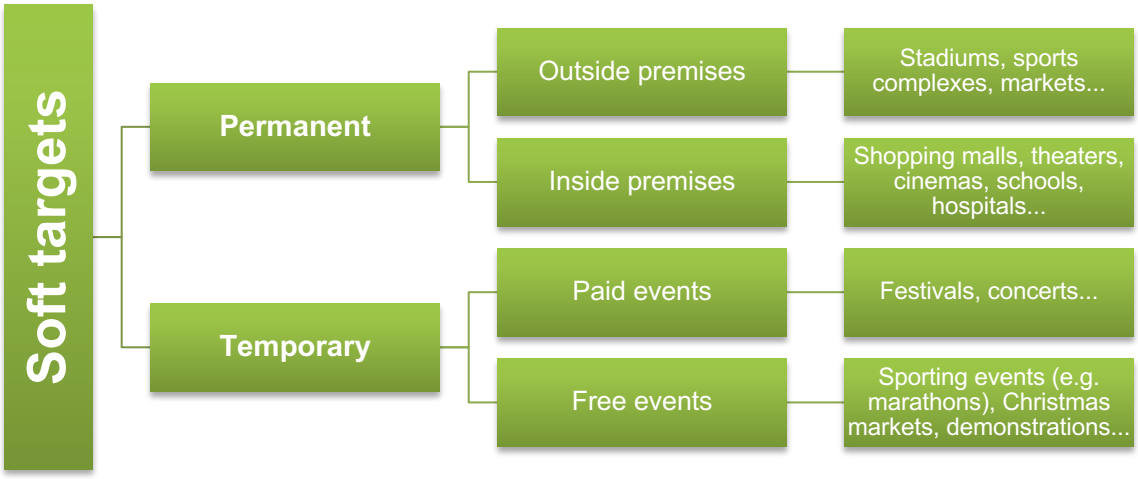


Figure 1 Soft targets according to the criterion of duration (according to: [15])

Given the significant vulnerability of soft targets, their protection is essential. Strategies for protecting soft targets can vary and will largely depend on the nature of the object, its security capabilities and on the financial resources of the given entity. Among the basic strategic directions of protection can be [15]:

- technical and technological measures and mechanical security devices, e.g., installation of security barriers, metal detectors, camera systems,
- regime measures,
- increased presence of security agencies,
- implementation of security procedures and training, e.g., regular training of personnel, students, pupils, etc. on how to respond to emergency situations, including evacuation plans and cooperation with law enforcement agencies,
- improving public awareness and involving the public in education about potential risks,
- ensuring inter-sectoral cooperation, e.g., coordination between the public and private sectors, security forces and local communities to improve information exchange and preparation for crisis situations,
- and other...

1.2 CRIME PREVENTION

Approaches in subchapter 1.1 essentially represent preventive measures in minimizing the occurrence of adverse events. Generally, this is addressed by crime prevention, which, according to [16] can be defined as follows: "Crime prevention encompasses all measures aimed at reducing or otherwise contributing to the reduction of crime and citizens' sense of insecurity, both

quantitatively and qualitatively, either by directly suppressing criminal acts or through policies and interventions aimed at reducing the potential for crime and the causes of crime. It includes the work of government, relevant authorities, criminal justice bodies, local authorities and specialized associations established in Europe, the private and voluntary sector, researchers and the public supported by the media."

The fundamental task of crime prevention is to help reduce the scope and severity of criminal and other antisocial activities to the greatest extent possible through the implementation of preventive activities, while simultaneously achieving an adequate increase in citizens' subjective sense of security and a reduction in the feeling of being threatened by crime. Thereby contributing to an improvement in the quality of life of society [17].

Crime prevention can be categorized according to multiple criteria. The fundamental division can be made based on specific preventive activities and the developmental stage of the criminal problem. The structure of this division is illustrated in Figure 2.

Figure 2 Structure of Crime Prevention (According to: [17])

Situational crime prevention holds a special position in the context of soft target protection [11, 17, 18, 19], which is specifically oriented towards crime, protection of public order, health, life and property of citizens by means of mechanical barriers, electrical security systems, physical protection and regime measures. The above activities assume that certain types of crime occur at certain times, places and circumstances. The essence of situational prevention is that, on the one hand, it makes it more difficult for a potential offender to commit a crime or other anti-social activity, and, on the other hand, it increases the likelihood of detecting the offender.

2 SITUATIONAL CRIME PREVENTION IN SCHOOLS AND SCHOOL FACILITIES

In the development and implementation of situational crime prevention measures, recommendations from the standard STN P CEN/TS 14383 Part 6 *Crime Prevention: Urban Planning and Design – Schools and Educational*

Institutions can be utilized. This standard represents one of the few official documents with a recommendatory nature that can serve as a basis for assessing and designing new situational crime prevention measures. **The primary objective** of the standard is to reduce risks associated with crime and antisocial behaviour committed against individuals and property in both private and public schools and educational institutions [19].

The examined standard provides a set of measures that can be implemented to reduce the risk of crime and other antisocial behaviour. It offers a comprehensive list of recommendations that takes a holistic approach to situational prevention. From this list, certain measures can be selected that would significantly contribute to enhancing security levels in schools. The selection is based on empirical experiences derived from collaboration with multiple schools. Based on the chosen recommendations, a checklist has been created to verify the implementation of measures at two selected schools in the city of Žilina. The assessment of these selected measures provides value to the participating schools, as the management is informed about potential vulnerabilities and identified risks that need to be mitigated. The selected measures derived from the examined standard, along with their compliance status at the two participating schools (S1 and S2), can be seen in Table 1.

Table 1 Selected Situational Prevention Measures and Assessment of Their Compliance in Schools

No.	Preventive measure according to STN P CEN/TS 14383-6	Compliance (✓/X)	
		S1	S2
1.	Has a risk assessment process been implemented and updated within the school?	X	X
2.	Does the school conduct regular (at least twice a year) training or education of employees in identifying and preventing crime and other antisocial activities?	X	X
3.	Does the school keep a record of security incidents?	✓	✓
4.	Are principles of safe behaviour and a list of items prohibited from being brought to school premises defined in the school rules?	✓	✓
5.	Is there a reception/front desk with permanent staff at the main entrance?	✓	✓
6.	Are the main entrances to buildings locked during teaching hours?	✓	✓
7.	Are pedestrian walkways built, maintained, and properly marked in the school grounds?	X	X
8.	Is the school property clearly separated and marked from publicly accessible space?	✓	X
9.	Is there signage about prohibited items at the entrance to the school grounds?	X	X

No.	Preventive measure according to STN P CEN/TS 14383-6	Compliance (✓/X)	
		S1	S2
10.	Is natural supervision ensured throughout the school grounds?	X	X
11.	Is the vegetation in the school grounds well-maintained?	X	✓
12.	Is there sufficient lighting in the school grounds?	X	X
13.	Is supervision by teaching staff carried out in corridors and classrooms during breaks?	✓	✓
14.	Are strangers (visitors) who enter the school grounds or buildings under constant supervision?	✓	✓
15.	Is there visible signage for buildings, rooms, classrooms, toilets, changing rooms... in the school grounds and buildings?	X	X
16.	There are no "blind" spots for youth gatherings in the school grounds (places where bullying, smoking, drinking alcohol... may occur)	X	X
17.	Are students, teaching staff, and parents properly informed about the school rules?	X	X

3 DISCUSSION AND CONCLUSION

The biggest shortcomings at both schools can be the lack of regular risk assessments along with a flexible response to modern threats. Staff tends to receive training in the form of distance learning to identify and manage selected phenomena - in particular bullying (according to interviews with teachers, this can be considered inappropriate and ineffective). Other socio-pathological phenomena and modern threats tend to be overlooked, and educators often fail to identify risky behaviour or signs of threats. Based on communication with educators and principals, education and awareness gaps can be seen in the areas of modern addictions (inability to identify tobacco products such as tobacco pouches, e-cigarettes or energy drinks), radicalisation (inability to identify right-wing or left-wing symbolism and inappropriate behaviours), eating disorders and self-harm. In addition to identification, there are no uniform procedures in schools to manage and prevent these specific phenomena, which often leads to them not being addressed.

The school grounds are maintained, but the signage and maintenance of pedestrian walkways is not in compliance with the requirements of the standard under review. There are also no pictograms at the entrances to the campus and school buildings indicating forbidden entry with selected items. These items are only defined in the school rules, which are located on visible spot in the main school building. The school rules can generally be considered as well drafted, but sufficient knowledge of contained information for pupils and parents is

questionable. Among the shortcomings of the school rules is the failure to define the access of persons to the school premises and buildings. This information does not need to be included in the school rules, but the information board at the entrance to the premises should clearly define the regime of access to schools and movement around buildings. From a personal experience, the "visitor" does not receive any information or rules for entry and movement around the campus or building upon entry.

In the school area natural supervision is mostly enabled, however, both schools have "blind spots" created by inadequately maintained greenery or barriers in the perimeter that do not allow for natural supervision over the entire area. Based on communication with educators, socio-pathological phenomena occur precisely in these "blind spots" – for example, the use of entertainment pyrotechnics of categories F2 and F3 (so-called firecrackers, whose main effect is noise), which is currently banned in Slovakia [20].

Based on the findings, it can be concluded that although schools are implementing some important security measures, there is considerable room for improvement. It is necessary to focus on:

- Implementation of regular and systematic risk assessments.
- Improving employee training in identifying and managing modern threats.
- Optimizing the school environment to eliminate "blind spots" and improve natural supervision.
- Improving the awareness of pupils, parents and visitors about security policies and procedures.

For the effective implementation of these measures, it would be appropriate to create a practical guide or methodology for school management and staff, which would assist them in planning and executing preventive measures. Such a document could be based on the standard STN P CEN/TS 14383-6 and should consider the specific conditions (cultural, social, economic, demographic…) of Slovak schools. Similar documents, methodologies, and guides exist, for example, in the Czech Republic. In the Czech Republic, there is a standard ČSN 73 4400 Prevention of Crime – Security Management in the Planning, Implementation, and Use of Schools and Educational Facilities. The standard is supplemented by a more detailed description and procedure for applying selected methods in the risk assessment process with illustrative examples. Additionally, clear methodologies, guides, and other practical materials intended for schools have been published for the Czech standard [21]. The development of similar practical documents could significantly strengthen the establishment of a safe and secure environment in schools in the Slovak Republic.

ACKNOWLEDGEMENT

The contribution was processed within the framework of the project APVV-23-0437 Stratégia a metodika ochrany mäkkých cieľov so zameraním na základné, stredné a vysoké školy.

LITERATURE

[1] TASR 2023. Vyšetrovanie vlaňajšej streľby na Zámockej ulici je vo finále, malo by byť skončené do mesiaca. Dostupné na internete: https://spravy.rtvs.sk/2023/10/vysetrovanie-vlanajsej-strelby-na-zamockej-ulici-je-vo-finale-malo-by-byt-skoncene-do-mesiaca/

[2] VRAŽDA, D. 2020. Pri útoku na základnej škole vo Vrútkach zomrel zástupca riaditeľky, útočník zranil aj deti. Polícia ho zastrelila. Dostupné na internete: https://dennikn.sk/1927282/utok-na-zakladnej-skole-vo-vrutkach/

[3] KYSEĽ, T. 2019. Devínsky masaker má päť rokov. Harman strieľal na všetko, čo sa hýbalo. Dostupné na internete: https://www.aktuality.sk/clanok/302968/foto-devinsky-masaker-ma-pat-rokov-harman-strielal-na-vsetko-co-sa-hybalo/

[4] *FN Brno se stala terčem kybernetického* útoku, 2020. Dostupné na internete: https://www.zdravotnickydenik.cz/2020/03/fn-brno-se-stala-tercem-kybernetickeho-utoku/

[5] TRANGEL, J. 2025. Všetko o hackerskom útoku na kataster: Prehľadné otázky a odpovede. Dostupné na internete: https://zive.aktuality.sk/clanok/D0efBvf/vsetko-o-hackerskom-utoku-na-kataster-prehladne-otazky-a-odpovede/

[6] MIHALKOVA, H. 2024. Do hybridnej vojny sú zatiahnuté aj školy, hovorí český odborník. Vysvetľuje, čo je cieľom hrozieb. Dostupné na internete: https://spravy.pravda.sk/domace/clanok/722628-rozhovor-libor-sladky-bombove-utoky-na-skoly-vyhrazky-cesko-skoly-maily/

[7] TASR, 2024. Šutaj Eštok oznámil, že na stovkách škôl nahlásili bombu. Polícia to vyšetruje ako teroristický útok. Dostupné na internete: https://www.ta3.com/clanok/955917/sutaj-estok-oznamil-ze-na-stovkach-skol-nahlasili-bombu-policia-to-vysetruje-ako-teroristicky-utok

[8] MIHÁLIKOVÁ, V. 2025. Nejde o nepopísaný list papiera, opísal generálny prokurátor Žilinka 18-ročného podozrivého z vražedného útoku na škole. 2025. Dostupné na internete: https://www.aktuality.sk/clanok/zgsE7KD/nejde-o-nepopisany-list-papiera-opisal-generalny-prokurator-zilinka-18-rocneho-podozriveho-z-vrazedneho-utoku-na-skole/

[9] *BIRÓ, M., ODKLADAL, M. 2023. Streľba v Prahe: Zbraň nájdená v dome strelca bola použitá v Klánovickom lese. Dostupné na internete: https://www.aktuality.sk/clanok/sNIUaZ6/strelba-v-prahe-zbran-najdena-v-dome-strelca-bola-pouzita-v-klanovickom-lese/*

[10] *Hospodářské noviny, 2023. Vláda na 23. prosince vyhlásila kvůli střelbě na filozofické fakultě státní smutek. Dostupné na internete: https://domaci.hn.cz/c1-67279130-vlada-na-23-prosince-vyhlasila-kvuli-strelbe-na-filozoficke-fakulte-statni-smutek*

[11] KALVACH, Z., et al. 2016. Basics of soft targets protection guidelines [online]. Praha: Soft Target Protection Institute, z.ú. Dostupné na internete:https://www.bing.com/search?q=%5B11%5D+KALVACH%2C+Z.%2C+et+al.+2016.+Basics+of+soft+targets+protection+guidelines+%5B&cvid=6739629c64e54325a51cb25573323ec0&gs_lcrp=EgRlZGdlKgYIABBFGDkyBggAEEUYOdIBBzQxMmowajSoAgiwAgE&FORM=ANAB01&PC=LCTS

[12] FOREST, J. F. 2006. Homeland Security: Protecting American‘s Targets. Greenwood. United States of America. ISBN ISBN 9780313054143

[13] HESTERMAN, J. 2014. Soft Target Hardering: Protecting People from Attack. New York: Routledge. ISBN 9780429256523

[14] KUBÍKOVÁ, Z. 2017. Identifikácia a hodnotenie mäkkých cieľov v lokálnom prostredí. In: Medzinárodný workshop - Bezpečnosť v lokálnom prostredí. Dostupné na internete: https://www.researchgate.net/publication/330738412

[15] APELTAUER, Tomáš et al. Ochrana měkkých cílů. Praha: Leges, 2019. ISBN 978-80-7502- 427-5.

[16] GAŠPIERIK, L. 2010. Prevencia criminality a inej protispoločenskej činnosti. Žilina: Multiprint s. r. o. 2010. ISBN 978-80-970410-0-7

[17] ŠOLTÉS, V. 2022. Kriminológia – Prevencia criminality a inej protispoločenskej činnosti v regiónoch Slovenska. Žilina: Edis, 2022. ISBN 978-80-554-1889-6

[18] CLARKE, R. V. 1995. Situational Crime Prevention. In: Crime and Justice, vol. 19. pp. 91–150. DOI https://doi.org/10.1086/449230

[19] STN P CEN/TS 14383 – 6 Predchádzanie zložinnosti. Územné plánovanie a navrhovanie budov. Časť 6: Školy a vzdelávacie inštitúcie

[20] Zákon č. 58/2014 Z. z. o výbušninách, výbušných predmetoch a munícii a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov.

[21] Asociace bezpečná škola z. s. 2019. *Pracovný list: Já a bezpečnost mé školy. Poznám varovné signály?* Praha: Asociace bezpečná škola z. s. 2019.

POŽIARNA OCHRANA VYBRANÝCH KULTÚRNYCH DREVENÝCH SAKRÁLNYCH PAMIATOK V OKRESE SOBRANCE

Michal Huliak[1], Iveta Marková[2]

ABSTRAKT

Kultúrne pamiatky majú významnú spoločenskú hodnotu. Zachovávajú rôzne umelecké štýly, ktoré sa vyvíjali v priebehu času, a mnohé z nich sa naďalej využívajú na pôvodné účely. Riziko vzniku požiaru je obzvlášť akútne pri stavbách postavených z horľavých materiálov. V tomto článku sa hodnotia súčasné protipožiarne opatrenia platné pre historické drevené sakrálne stavby v okrese Sobrance. Na zber údajov sa použil kontrolný zoznam a zistenia sa analyzovali s cieľom určiť opakujúce sa nedostatky. Ako hlavné nedostatky v oblasti protipožiarnej ochrany boli identifikované: absencia protipožiarnych náterov, nefunkčné systémy elektrickej požiarnej signalizácie a chýbajúce stabilné hasiace systémy. Okrem toho bola problematická aj prítomnosť horľavých materiálov v budovách a ich okolí, dostupnosť vodných zdrojov, primeranosť prístupových ciest a reakčný čas hasičského zboru. Riešenie týchto problémov, najmä inštalácia funkčnej elektrickej signalizácie, má zásadný význam pre zlepšenie požiarnej ochrany. Nedostatok finančných prostriedkov však predstavuje hlavnú prekážku pri realizácii týchto potrebných zlepšení, čím sa ohrozuje zachovanie týchto kultúrnych pamiatok.

Kľúčové slová:
Protipožiarna ochrana, historické drevo, drevené kostoly, kultúrne pamiatky, fire risk assessment

ABSTRACT

Heritage buildings have significant social value. They preserve a variety of artistic styles that have evolved over time, and many continue to be used for their original purposes. The risk of fire is particularly acute in buildings constructed of combustible materials. This article assesses the current fire protection measures in place for heritage timber religious buildings in the

1 Michal Huliak, Ing., Žilinská univerzita, Fakulta bezpečnostného inžinierstva, Katedra požiarneho inžinierstva, Ul. 1.mája Žilina 01026, tel: 041 513 6769, E-mail: michal.huliak@uniza.sk
2 Iveta Marková, prof., RNDr., PhD., Žilinská univerzita, Fakulta bezpečnostného inžinierstva, Katedra požiarneho inžinierstva, Ul. 1.mája Žilina 01026, tel: 041 513 6799 E-mail: iveta.markova@uniza.sk

Sobrance district. A checklist was used to collect data and the findings were analysed to identify recurring deficiencies. The main deficiencies in the area of fire protection were identified as: the absence of fire protection coatings, non-functioning electrical fire alarm systems and the absence of stable fire extinguishing systems. In addition, the presence of combustible materials in and around buildings, the availability of water sources, the adequacy of access routes and the response time of the fire brigade were also problematic. Addressing these issues, particularly the installation of functional electrical alarms, is essential to improving fire protection. However, the lack of funding is a major obstacle to the implementation of these necessary improvements, thus jeopardizing the preservation of these heritage buildings.

Key words:
Fire protection, ancient timber, timber churches, heritage buildings, fire risk assessment

1 ÚVOD

Na slovenskom vidieku bolo drevo až do druhej polovice 20. storočia prevládajúcim stavebným materiálom. Jeho rozšírené používanie sa pripisovalo jeho ľahkej dostupnosti a nižšej cene v porovnaní s alternatívnymi materiálmi, ako sú kameň a tehla. Kamenné a tehlové stavby boli zvyčajne vyhradené pre mestské prostredie alebo sídla bohatších jednotlivcov. Prevaha dreva v dedinskej výstavbe však znamenala aj to, že celé dediny boli náchylné na zničenie požiarom. Prijatie modernejších stavebných techník a materiálov viedlo k výstavbe nových náboženských budov s využitím týchto vymožeností, čo často viedlo k zbúraniu starších, menej hodnotných drevených stavieb. Napriek tomu mnohé drevené náboženské stavby pretrvali mnoho storočí.

Prvé snahy o ochranu pamiatok v našom regióne, ktoré sa začali koncom 19. storočia, spočiatku ľudovú architektúru prehliadali. Až po vzniku Československa sa drevenej architektúre, najmä kostolom na Slovensku, začala venovať sústredená pozornosť, ktorá viedla k vytvoreniu súpisov kultúrnych pamiatok a k aktívnym ochranárskym opatreniam [1].

Tieto kultúrne pamiatky, ktoré majú zásadný význam pre naše kultúrne dedičstvo, sú jedinečne zraniteľné požiarom. Ako upozorňuje Torero [2], moderné bezpečnostné normy nemožno na tieto stavby plne aplikovať bez toho, aby sa narušila ich historická integrita. V dôsledku toho musia stratégie ochrany a uchovávania pamiatok uprednostňovať protipožiarnej ochranu. Vzhľadom na ich spoločenský význam je okamžitá detekcia a likvidácia požiaru kľúčová pre ochranu týchto nenahraditeľných stavieb.

Historické drevené kostoly, hoci sú kultúrne významné, sú mimoriadne zraniteľné voči požiarom. Prirodzená horľavosť ich drevenej konštrukcie je znásobená ich častým umiestnením v odľahlých oblastiach, kde sú prístup a vodné zdroje často nedostatočné na účinné hasenie ako bolo zmienené v [3].

Nevyhnutnosť protipožiarnych náterov s ich obmedzenou životnosťou 10 až 15 rokov ešte viac zvýrazňuje neustále problémy pri ochrane týchto nenahraditeľných stavieb.

Výskum [4] preukázal účinnosť ošetrenia dreva v protipožiarnej ochrane. Porovnaním ošetreného a neošetreného dreva sa zistilo, že ošetrenie predĺžilo odolnosť proti šíreniu plameňa z 52 sekúnd na 570 sekúnd. Toto výrazné zvýšenie podčiarkuje kľúčovú úlohu protipožiarnej ochrany pri ochrane drevených konštrukcií.

V dokumente [5] sa uvádza niekoľko zraniteľných miest, ktoré sú spoločné pre historické drevené stavby, vrátane absencie elektrickej požiarnej signalizácie, nedostatočného počtu hasiacich prístrojov, nedostatočného osvetlenia, obmedzených zásob vody a chýbajúcej ochrany pred bleskom. Poľský národný výbor ICOMOS [6] okrem toho upozorňuje na ďalšie riziko podpaľačstva pri krádežiach, keď sa oheň využíva na zakrytie trestného činu.

Hlavnou výzvou je nájsť rovnováhu medzi zvýšením požiarnej bezpečnosti a zachovaním historickej integrity. Zavádzanie moderných protipožiarnych opatrení je často v rozpore so smernicami pamiatkovej ochrany, ktorých cieľom je zabrániť viditeľným zmenám charakteru budovy. V dôsledku toho sa mnohé pasívne protipožiarne systémy a vytváranie nových únikových ciest považujú za nevhodné. Ako sa zdôrazňuje v [7], je nevyhnutné nájsť kompromis medzi bezpečnosťou a ochranou pamiatok.

Severské krajiny, najmä Nórsko, demonštrujú holistický prístup k ochrane historických drevených budov, ktorý rozširuje požiarnu ochranu nad rámec samotnej stavby na jej okolité prostredie. To zahŕňa manažment vegetácie, zlepšenie zásobovania vodou a komunitné protipožiarne cvičenia [8]. Koncepcia ochrany okolia, ako sa uplatňuje na drevené dediny v [8], je relevantná aj pre izolované historické budovy v blízkosti obytných oblastí. Často sa odporúčajú riešenia aktívnej požiarnej ochrany, ako sú požiarne hlásiče, infračervené kamery na monitorovanie obvodu a stacionárne sprinklerové systémy.

Dilemu predstavuje voľba medzi vodnými a plynovými hasiacimi systémami. Systémy vodných clôn [9] ponúkajú účinnú ochranu s minimálnym zmáčaním stien, ale v nevykurovaných budovách čelia problémom kvôli riziku zamrznutia. Suché systémy sú menej účinné. Plynové hasiace systémy minimalizujú škody v interiéroch, ale sú nákladné a nevhodné na vonkajšiu ochranu, pričom predstavujú aj riziká pre obyvateľov a hasičov.

Na našom území sa nachádza 59 drevených kostolov, ktoré patria medzi kultúrne pamiatky, vrátane ôsmich pamiatok zapísaných na zozname svetového dedičstva UNESCO [13]. Hoci sa projekt „Záchrana drevených kostolov“ z roku 2010 zaoberal rekonštrukciou a niektorými protipožiarnymi opatreniami (protipožiarne nátery, hasiace prístroje a elektrické systémy), protipožiarna

ochrana je v našej oblasti stále kriticky málo preskúmaná. Náš výskum zistil výrazný nedostatok odborných zdrojov venovaných tejto problematike. Tieto nenahraditeľné stavby postavené z vysoko horľavých materiálov sú zraniteľné voči nezvratným škodám. Ich architektonický, umelecký a náboženský význam zdôrazňuje naliehavú potrebu špecializovaných stratégií požiarnej bezpečnosti.

2 METODOLÓGIA

Cieľom nášho výskumu bolo posúdiť požiarnu bezpečnosť historických drevených kostolov na východnom Slovensku, čo si vzhľadom na ich jedinečné vlastnosti vyžaduje diferencovaný prístup. Na dosiahnutie tohto cieľa sme použili kvalitatívnu metódu zberu údajov s využitím vlastného kontrolného zoznamu. Tento prístup bol zvolený s cieľom zabezpečiť dôkladné preskúmanie každého objektu, čo umožnilo identifikovať kritické slabé miesta požiarnej bezpečnosti a zároveň zmierniť potenciálne nepresnosti údajov, ktoré sú vlastné rozsiahlym prieskumom [14].

Pri vypracovaní kontrolného zoznamu sa vychádzalo z komplexného prehľadu príslušnej literatúry [1 - 13], ktorý poukázal na špecifické požiarne riziká spojené s týmito stavbami. Prevzali sme aj prvky z metodiky hodnotenia požiarnej ochrany pamiatok českého Národného pamiatkového ústavu [15], ktorá poskytla cenný rámec na kategorizáciu kľúčových parametrov požiarnej bezpečnosti. Medzi tieto kategórie patril materiál a vek budovy, použitie protipožiarnych látok, elektrické a bleskozvodné systémy, prítomnosť a funkčnosť hasiacich prístrojov a alarmov, dostupnosť vody, prístup záchranných služieb a plánovanie evakuácie. Kombináciou poznatkov z existujúceho výskumu so zavedenými hodnotiacimi protokolmi sme mohli vytvoriť kontrolný list na hodnotenie požiarnej bezpečnosti týchto historicky a kultúrne významných budov, ktorý je prispôsobený na mieru.

Na posúdenie požiarnej bezpečnosti sa údaje zbierali v januári 2024, čo je obdobie zvolené tak, aby odrážalo sezónne zmeny dostupnosti. Použil sa štruktúrovaný kontrolný zoznam, ktorý obsahoval binárne (áno/nie) aj kvantitatívne (číselné) otázky, určené na komplexné zhodnotenie špecifík súvisiacich s požiarmi. Témy a špecifiká z požiarneho hľadiska boli zahrnuté v kontrolnom zozname:

- Typ stavebného podkladu, Izolácia, Hromozvod
- Protipožiarny náter,
- Elektrická požiarna signalizácia,
- Stabilné hasiace zariadenie,
- Prenosné hasiace prístroje

Objekty boli vybrané vo východnej časti Slovenska, v okrese Sobrance. Išlo o 4 drevené chrámy Chrám Prenesenia relikvií svätého Mikuláša v Ruskej Bystrej, Chrám svätého Michala archanjela v Inovciach, Chrám svätého Bazila

Veľkého v Hrabovej Roztoke a Chrám Nanebovstúpenia Pána v Šmigovci. Chrám v Ruskej Bystrej je zapísaný v zozname UNESCO.

Obrázok 1 Chrám Prenesenia relikvií svätého Mikuláša v Ruskej Bystrej; Chrám svätého Michala archanjela v Inovciach; Chrám svätého Bazila Veľkého v Hrabovej Roztoke; Chrám Nanebovstúpenia Pána v Šmigovci

3 VÝSLEDKY

Drevené sakrálne stavby

Chrámy boli postavené v rokoch 1730 (Ruská Bystrá), 1750 (Hrabová Roztoka), 1755 (Šmigovec) a 1836 (Inovce). Každý chrám má ako stavebný základ kameň, pričom pôvodne bolo ako stavebný základ použité drevo zapustené do zeme. Kamenný základ tvorí aj chodník okolo stavieb, ktorého priemerná šírka je 50 cm. Obloženie chrámov bolo riešené položením dreva tak, aby nevznikali medzery, a preto pri chrámoch v Hrabovej Roztoke a Šmigovci nebolo potrebné vyplnenie. V dvoch prípadoch (Ruská Bystrá a Inovce) bola ako izolácia použitý mach.

Protipožiarny náter

Protipožiarny náter bol aplikovaný na 3 chrámy, chýbal na chráme v Hrabovej Roztoke. V chráme v Šmigovci bola v interiéri použitá omietka, aj v tomto objekte bol aplikovaný protipožiarny náter. Protipožiarny náter bol aplikovaný v rokoch 2007 až 2014. Priemerná životnosť protipožiarneho náteru je 10 až 15 rokov, čo je pre tento typ stavby krátka doba.

Elektrická požiarna signalizácia

Vo všetkých budovách bola nainštalovaná elektrická požiarna signalizácia. V troch z nich nefungovala, bola ručne odpojená, pretože počas

užívania budovy spúšťala falošné poplachy. V chráme v Hrabovej Roztoke bola funkčná. Vo všetkých budovách boli opticko-dymové hlásiče. Výstup zo systému elektrickej požiarnej signalizácie bol vo forme zvukového signálu poplachu z budovy. Signál z elektrickej požiarnej signalizácie nebol odoslaný na ústredňu Hasičského záchranného zboru.

Hasiace prístroje

Prenosné hasiace prístroje boli nainštalované v troch budovách, v chráme v Šmigovci chýbajú. V dvoch budovách bol jeden hasiaci prístroj s práškovým hasiacim prostriedkom a v chráme v Inovciach dva práškové hasiace prístroje.

Stabilné hasiace zariadenie

V žiadnej z kontrolovaných budov nebolo nainštalované stabilné hasiace zariadenie. V chráme v Ruskej Bystrej, ktorý je na zozname UNESCO, nám bolo povedané, že sa plánuje inštalácia stabilného hasiaceho systému s hasiacou látkou plynom. Bližšie informácie o plánovanom projekte sme nezískali.

4 DISKUSIA

Z výsledkov, ktoré sme zistili, vyplýva niekoľko zistení, ale aj nedostatkov, ktoré je potrebné odstrániť alebo vytvoriť podmienky na ich odstránenie. Pozitívnym zistením bolo, že každý z objektov má kamenný základ. Drevo sa nedotýka zeme a nehrozí jeho degradácia spôsobená škodcami alebo zemnou vlhkosťou. Taktiež v prípade, že by došlo k požiaru niektorého zo stromov v blízkosti budovy a k rozšíreniu požiaru koreňmi, stavby by boli pred týmto vplyvom chránené.

Pri protipožiarnom nátere sa zistilo, že ho majú nanesený 3 objekty. Chrám v Hrabovej Roztoke ho však nemal a tie, na ktorých sa nachádza, už majú podľa odhadu priemernej časovej účinnosti uplynutú dobu platnosti. Bolo by preto potrebné zabezpečiť protipožiarny náter aspoň na tých objektoch, kde nebol aplikovaný. Pri ďalšej rekonštrukcii alebo oprave častí budov by bolo vhodné, keby sa uvažovalo aj o protipožiarnych náteroch. Problémom je, že niektoré budovy majú na vnútornej strane stien maľby, ktoré vzhľadom na ich historickú a náboženskú hodnotu nemožno natrieť protipožiarnym náterom, pretože by mohlo dôjsť k ich poškodeniu alebo znehodnoteniu, čo by pamiatkový úrad neschválil.

Elektrickú požiarnu signalizáciu považujeme za jeden z najdôležitejších prvkov pasívnej požiarnej ochrany. Ak sa požiar zistí včas, môže zachrániť väčšiu časť budovy alebo uhasiť požiar skôr, ako stihne poškodiť vnútorné zariadenie budovy. Preto považujeme za negatívne zistenie, že bol funkčný len v chráme v Hrabovej Roztoke. Najmä v nočných hodinách, keď je v okolí budovy znížená aktivita, je to jediná možnosť, ako požiar včas spozorovať. Vhodným riešením situácie by bolo nahlásenie výjazdu zodpovednej osobe z obce a na najbližšiu hasičskú stanicu. Tým by sa skrátil reakčný čas a čas rozvoja požiaru,

čo by mohlo viesť k záchrane pamiatky. Na zvýšenie požiarnej ochrany by bolo dôležitým faktorom vybavenie ostatných budov, v ktorých nie je elektrická požiarna signalizácia. Taktiež v tých budovách, kde bola odpojená alebo nefungovala z iných dôvodov, aby sa mohla opraviť a nefunkčné hlásiče vymeniť. Ide o finančne náročné opatrenie, preto by bolo vhodné, keby sa na jeho financovanie podarilo získať sponzorov, prípadne Ministerstvo kultúry SR alebo prostriedky z Európskej únie. Ďalšou možnou inštitúciou, ktorá by mohla pomôcť s financovaním, je ICOMOS, Medzinárodná rada pre pamiatky a sídla, ktorá sa venuje zachovaniu a ochrane pamiatok. V roku 2022 bolo na tento typ objektov na Ukrajine dodaných 440 vodných prenosných hasiacich prístrojov, čo dokazuje záujem spoločnosti o ochranu historických drevených sakrálnych stavieb [16].

Priaznivým zistením bola prítomnosť hasiacich prístrojov, s výnimkou jedného chrámu v Šmigovci. Po kontrole a komunikácii so zodpovednými správcami objektov bolo odporučené vybaviť aj tento objekt prenosným hasiacim prístrojom, čo malo kladnú odozvu. V tých objektoch, kde je len jeden hasiaci prístroj, by sa mohol osadiť ešte jeden hasiaci prístroj, ktorý by bol umiestnený pri vstupe do objektu a na najvzdialenejšom mieste od vstupu. Pomocou hasiacich prístrojov je možné uhasiť požiar v jeho iniciačnej fáze.

V žiadnej zo skúmaných budov sa nenachádza stabilné hasiace zariadenie. Ide o finančne najväčšiu položku z hľadiska požiarnej ochrany. Finančne by sa to mohlo riešiť rovnakým spôsobom ako v prípade elektrickej požiarnej signalizácie.

To vyvoláva otázku inštalácie stabilného hasiaceho zariadenia s vhodným hasiacim prostriedkom. Plynom poháňané stabilné hasiace zariadenie sa môže inštalovať len na ochranu interiéru budovy, zatiaľ čo systém s vodným hasiacim prostriedkom sa môže inštalovať na ochranu interiéru aj plášťa budovy. Nevýhodou vodného hasiaceho prostriedku je, že by mohol poškodiť interiér budovy. Vhodným riešením z nášho pohľadu by bola inštalácia vodnej clony s úpravou tak, aby trysky nedodávali vodu na steny budovy, ako sa uvádza v [8]. Ak by sa inštalácia uskutočnila, vznikla by ďalšia otázka, aký typ použiť, či mokrý alebo suchý systém, pretože voda v potrubí by mohla v zime zamrznúť. Uprednostňoval by sa suchý systém, hoci by sa tým predĺžil čas začatia hasenia, znížilo by sa riziko zamrznutia vody v potrubí a účinnosť hasenia by bola neúčinná.

5 ZÁVER

Nastavenie požiarnej ochrany drevených sakrálnych stavieb je komplikované, predovšetkým kvôli rozporu medzi snahou o zachovanie architektonického vzhľadu a nutnosťou implementácie moderných bezpečnostných opatrení. Nájsť prijateľný kompromis medzi potrebami komunity usilujúcej o uchovanie historického charakteru a požiadavkami na

zaistenie požiarnej bezpečnosti je zásadné. Hoci moderné technológie ponúkajú nové možnosti ochrany, ich implementácia často naráža na vysoké finančné náklady. Naša analýza identifikovala pozitívne aj negatívne aspekty existujúcich opatrení. Medzi pozitíva patrí použitie nehorľavých materiálov na stavebných základoch, možnosť odstránenia horľavých materiálov z bezprostredného okolia budov a prítomnosť hasiacich prístrojov s výnimkou jedného objektu.

Zistili sme viacero negatívnych skutočností, kde elektrická požiarna signalizácia bola funkčná len v jednej budove, v žiadnej budove nie je stabilné hasiace zariadenie, na troch budovách boli použité protipožiarne nátery, z ktorých mnohé už boli po predpokladanej životnosti.

Celkovo sa ukázalo, že stav protipožiarnej ochrany drevených sakrálnych stavieb v okrese Sobrance má nedostatky a rozdiely, ktoré je možné riešiť. Doplnenie vybavenia a realizácia opatrení by pomohli k ochrane týchto objektov a ich zachovaniu pre budúce generácie.

POĎAKOVANIE

Za umožnenie obhliadky chrámov sa chceme poďakovať vlastníkovi objektov v obciach Inovce, Hrabová Roztoka a Šmigovec, ktorým je Gréckokatolícke arcibiskupstvo Prešov. Poďakovať chceme aj vlastníkovi objektu v obci Ruská Bystrá, ktorým je Michalovsko-košická pravoslávna eparchia.

LITERATÚRA

[1] “Dejiny pamiatkovej starostlivosti” Pamiatkový úrad Slovenskej republiky. Dostupné na: https://www.pamiatky.sk/ochrana-pamiatok/dejiny-pamiatkovej-starostlivosti/

[2] José L. Torero (2019) “Fire Safety of Historical Buildings: Principles and Methodological Approach”. International Journal of Architectural Heritage, 13:7, 926-940, DOI: 10.1080/15583058.2019.1612484

[3] Kozłowski, R. (2015) “Wooden heritage buildings and preventing them against fire”, Budownictwo i Architektura, 14(4), pp. 079–087. doi: 10.35784/bud-arch.1538.

[4] Tsapko, J., Bondarenko, O., Tsapko, A., Gorbachova, A. Yu., Mazurchuk, S., Zherebchuk, D., “JUSTIFICATION OF THE EFFICIENCY OF FLOATING COATING FOR FIRE PROTECTION OF WOODEN BUILDINGS. Modern construction and architecture, 2023, no. 3, page 49-60. DOI:10.31650/2786-6696-2023-3-49-60

[5] Vovk S., Ferents N., Lyn A., “RELIGIOUS BUILDINGS FIRE SAFETY IN UKRAINE.” Fire Safety, No37, 2020. DOI:10.32447/20786662.37.2020.04 ISSN 2708-1087

[6] “Dangers to the Sacred Wooden Architecture in Poland.” HERITAGE AT RISK. ICOMOS World Report 2002-2003 on monuments and sites in

danger. Dostupné na: https://www.icomos.org/public/risk/2002/poland2002.htm
[7] Quapp, U., Holschemacher K., “Heritage Protection Regulations in Germany and their Relations to Fire Safety Demands.” 2020 IOP Conf. Ser.: Mater. Sci. Eng. 753 042036 DOI 10.1088/1757-899X/753/4/042036 Dostupné na:
[8] Kristoffersen M., Log T., “Experience gained from 15 years of fire protection plans for Nordic wooden towns in Norway.” Safety Science Volume 146, February 2022, 105535. Dostupné na: https://www.sciencedirect.com/science/article/pii/S0925753521003787
[9] Jensen, Geir, ”A White paper on Water Mist for Protection of Heritage”, Interconsult ASA, July 12, 2004. The report may be downloaded from www.heritagefire.net/ or www.iwma.net/. Dostupné na: https://sprinklerframjandet.se/wp-content/uploads/Water_Mist_in_Heritage_Report_Complete_Cover.pdf
[10] Arvidson M., “An overview of fire protection of Swedish wooden churches.” SP Swedish National Testing and Research Institute. SP Fire Technology SP REPORT 2006:42. Dostupné na: https://www.diva-portal.org/smash/get/diva2:962374/FULLTEXT01.pdf
[11] Kincaid S., “Fire prevention in historic buildings – approaches for safe practice.” THE HISTORIC ENVIRONMENT: POLICY & PRACTICE 2022, VOL. 13, NO. 3, 361–380 Dostupné na: https://www.tandfonline.com/doi/epdf/10.1080/17567505.2022.2098633?needAccess=true
[12] Historic Scotland, Fire Protection and the Built Environment: Conference Proceedings. 1999. Edinburgh, Historic Scotland
[13] Kurilcová, A., “Gréckokatolícka cirkev na Slovensku po roku 1989 a jej rozvoj v oblasti architektúry” Prešovská univerzita v Prešove. 2015 Dostupné na: https://www.pulib.sk/web/kniznica/elpub/dokument/novakova1/subor/Kurilcova.pdf
[14] Higgins, W. Y., Boorman, D. J., “An analysis of the effectiveness of checklists when combined with other processes, methods and tools to reduce risk in high hazard activities.” 2016. Boeing Technical Journal. Dostupné na: http://www.boeing.com/resources/boeingdotcom/specialty/innova-tion-quarterly/December-2016/BTJ_Checklist_full.pdf
[15] Jirásek, P., Mrázek, M., Polatová E., Svoboda, P., “Požární ochrana památkových objektů.” Praha. Národní památkový ústav. 2014 ISBN 978-80-7480-021-4
[16] “The Foundation to Preserve Ukraine’s Sacral Arts, ICOMOS and World Monuments Fund deliver fire extinguishers to protect Ukraine’s wooden churches.” 2022. Available at : https://www.icomos.org/images/DOCUMENTS/Secretariat/2022/Ukraine/FTPUSA-ICOMOS-WMF_release_EN_final20220711.pdf

DÁTOVÝ RÁMEC POSUDZOVANIA RIZÍK PREPRAVY NEBEZPEČNÝCH LÁTOK CESTNOU DOPRAVOU A NÁVRH KONCEPTU ECALL PRE PODPORU ZÍSKAVANIA INFORMÁCIÍ V REÁLNOM ČASE

Boris Kollár[1], Daniel Chovanec[2] a Karin Nováková[3]

ABSTRAKT

Preprava nebezpečných látok cestnou dopravou predstavuje významné riziká pre obyvateľstvo a životné prostredie. Príspevok identifikuje a kategorizuje premenné potrebné pre posudzovanie rizík prepravy nebezpečných látok a analyzuje ich možné využitie v podpore rozhodovania počas havárií. Tieto údaje je možné využiť na tvorbu modelov, simulácií alebo scenárov v predkrízovej fáze, ako aj na podporu zásahových zložiek počas reakcie na krízové javy. Zároveň je navrhnutý koncept rozšíreného systému eCall pre nákladné vozidlá prevážajúce nebezpečné látky, ktorý by do minimálneho súboru údajov integroval dôležité informácie o druhu a množstve prepravovanej nebezpečnej látky v reálnom čase.

Kľúčové slová:
Manažment rizík, posudzovanie rizík, preprava nebezpečných látok, dátová podpora, eCall.

ABSTRACT

Transport of dangerous substances by road poses significant risks to the population and the environment. The paper identifies and categorizes the variables needed for assessing the risks of dangerous substances transport and analyzes their possible use in decision support during accidents. This data can be used to create models, simulations or scenarios in the pre-crisis phase, as well as to support emergency responders during crisis response. At the same time, the concept of an enhanced eCall system for trucks carrying dangerous goods is proposed, which would integrate into a minimal data set important real-time information on the type and quantity of dangerous goods being transported.

1 Ing. Boris Kollár, Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, 1. mája 32, 01026 Žilina, Slovensko, boris.kollar@uniza.sk
2 Ing. Daniel Chovanec, Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, 1. mája 32, 01026 Žilina, Slovensko, daniel.chovanec@uniza.sk
3 Ing. Karin Nováková, Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, 1. mája 32, 01026 Žilina, Slovensko, Novakova@naw.sk

Key words:
Risk management, risk assessment, transport of dangerous substances, data support, eCall.

1 ÚVOD

Cestná doprava je najvýznamnejším druhom dopravy v podmienkach Európskej únie. Jej vplyv na ekonomiku a hospodárstvo jednotlivých krajín ju predurčuje byť jedným z kľúčových odvetví kritickej infraštruktúry [1]. Práve jej význam pre hospodárstvo, spoločnosť ale i zložky integrovaného záchranného systému (ďalej IZS), určuje potrebu jej ochrany, pričom jednou z hlavných oblastí tejto ochrany je riadenie rizík [2]. Súčasťou riadenia rizík je ich posudzovanie, ktoré sa skladá z ich identifikácie, analýzy a hodnotenia [3]. Okrem riadenia a posudzovania rizík sa v literatúre často stretávame s posudzovaním zraniteľnosti alebo odolnosti prvkov kritickej infraštruktúry [1], [4], [5]. Pre tento účel sa rovnako ako v iných oblastiach využívajú rôzne parametre a premenné.

Tieto parametre sú často krát základnými údajmi, ktoré vstupujú do procesu posudzovania rizík. Okrem prítomnosti rizika narušenia cestnej infraštruktúry, existuje riziko spojené s jej využívaním. Ide najmä o prepravu nebezpečných látok (ďalej NL), ktoré môžu v prípade úniku spôsobiť vážne negatívne následky na obyvateľstve a životnom prostredí [6]. Limitovať ich pôsobenie je veľmi dôležité a je potrebná včasná reakcia príslušných orgánov ale i zasahujúcich jednotiek, ktoré musia aplikovať vhodné sorpčné prostriedky a iné opatrenia [7]. Včasnosť a presnosť údajov a informácií je preto kľúčovým predpokladom úspešnej reakcie na vzniknutý krízový jav.

Posúdenie rizika prepravy NL vo všetkých druhoch dopravy je v podmienkach Slovenskej republiky (SR) súčasťou Analýzy územia z hľadiska vzniku možných mimoriadnych udalostí (ďalej Analýza územia). Obsahová analýza týchto dokumentov a identifikované problémy počas konzultácií na odboroch krízového riadenia okresných úradov na tému spracovania a využitia Analýzy územia, poukázali na nedostatky v tejto oblasti. Posúdenie rizika prepravy NL je v súčasnosti obmedzené na identifikáciu ciest, po ktorých by sa tieto NL mohli prepravovať, a obcí, cez ktoré tieto cesty vedú. Problémom je najmä:

- nedostupnosť potrebných údajov,
- nedostupnosť softvérových nástrojov
- a nedostupnosť metodického postupu alebo metódy na posúdenie tohto typu rizika [8-12].

2 IDENTIFIKÁCIA HLAVNÝCH KATEGÓRIÍ A ICH PREMENNÝCH PRE POSÚDENIE RIZIKA PREPRAVY NEBEZPEČNÝCH LÁTOK

Havária nákladného vozidla spojená s únikom NL môže ohroziť samotnú cestnú komunikáciu, spomaliť alebo úplne zastaviť dopravu a najmä ohroziť obyvateľov a životné prostredie. Ide o komplexnú problematiku, pričom však podľa autorov Liu a kol. [6], sa väčšina modelov posúdenia rizika alebo ich hodnotenia, zameriava na stanovenie následkov na obyvateľstve. Komplexný prístup v tejto oblasti zaujali autori Huang a kol. [13], ktorí na posúdenie rizika prepravy NL v území využili súbory viacerých údajov na reprezentáciu kľúčových premenných. Kombináciou údajov o predchádzajúcich nehodách, údajoch o NL a území, vytvorili model, ktorý kategorizuje jednotlivé druhy NL a dokáže odhadnúť predpokladaný rozsah úniku podľa meteorologických charakteristík sledovaného územia.

Vzhľadom na identifikáciu kategórií a ich premenných, potrebných na posúdenie rizík prepravy NL, je možné vychádzať zo štúdie od autorov Kubás a kol., [14] ktorí okrem vstupných premenných popísali tiež postup výpočtu rozsahu úniku pomocou softvérového nástroja. Pre posúdenie rizika úniku NL sú softvérové nástroje kľúčovým predpokladom kvalitného výstupu. Tieto nástroje sú však dôležité tiež v prípade rýchlej a efektívnej reakcie pozostávajúcej z rozhodnutí založených na presných a včasných informáciách [15]. Analýzou ďalších relevantných štúdií a dokumentov boli identifikované a následne kategorizované hlavné premenné potrebné na dôkladné posúdenie rizika. Tieto premenné sú uvedené v nasledujúcej tabuľke 1.

Tabuľka 1 Vstupné premenné pri posudzovaní rizika prepravy nebezpečných látok (vlastné spracovanie na základe: [8-11], [13], [14], [16-19]

Kategória	Meteorologické údaje	Údaje o NL	Územné a demografické údaje	Údaje o cestnej sieti	Historické údaje
Premenné	*-rýchlosť vetra* *-smer vetra* *-vertikálna stabilita vzduchu* *-teplota vzduchu* *-výška meracích zariadení* *-povaha počasia*	*-názov NL* *-UN kód* *-Kemler kód* *-ADR trieda* *-GHS Hazard Statements* *-množstvo NL* *-údaje o poskytovateľovi* *-údaje o prijímateľovi*	*-počet obyvateľov* *-vrstva objektov* *-vrstva vodných plôch a tokov* *-vrstva národných parkov a chránených oblastí*	*-vrstva cestnej siete* *-rozdelenie ciest* *-cestné obmedzenia* *-vyťaženosť cestnej siete*	*-čas havárie* *-názov NL* *-množstvo uniknutej NL* *-lokácia havárie* *-počet zasiahnutých osôb* *-zasiahnuté: vodné zdroje, plochy, chránené územia, ...*

Uvedené kategórie a ich premenné tvoria základnú bázu dát pre komplexné posúdenie rizika prepravy NL. Ich prepojením, analýzou a s využitím softvérových nástrojov je možné s pomocou geografických informačných systémov (GIS) vizualizovať potenciálne úniky, identifikovať ohrozené časti obcí

a vypočítať počet ohrozených obyvateľov alebo definovať ohrozenie životného prostredia. Doplňujúce údaje následne umožnia charakterizovať charakter NL a prijať adekvátne opatrenia pre krízové štáby a zasahujúce jednotky IZS.

Problémom je však identifikácia a zber údajov a informácií v reálnom čase. Analýzou a následnou syntézou uvedených údajov je možné vytvoriť scenáre havárií pre jednotlivé cestné úseky alebo obce, čo v prípade reakcie poskytne kompetentným orgánom približné informácie o priebehu a následkoch mimoriadnej udalosti. Pre presnejšie informácie je však potrebné zabezpečiť, aby vybrané údaje z tabuľky č. 1, boli dostupné v reálnom čase. Práve túto problematiku rozoberá navrhnutý koncept eCall-u pre nákladné vozidlá prepravujúce NL.

3 NÁVRH KONCEPTU ECALL PRE NÁKLADNÉ VOZIDLÁ PREPRAVUJÚCE NEBEZPEČTNÉ TOVARY V CESTNEJ DOPRAVE

Hlavnou úlohou eCall-u, je v prípade nehody, spojiť vozidlo s operačným strediskom IZS. Najdôležitejším cieľom systému eCall je skrátiť reakčný čas záchranných služieb, a tým znížiť počet úmrtí a následkov nehôd [20]. Od 31.3.2018 je zariadenie eCall na základe Nariadenia Európskeho parlamentu a Rady (EÚ) 2015/758 o požiadavkách typového schválenia pri zavádzaní palubného systému eCall využívajúceho službu tiesňovej linky 112, povinné pre všetky vozidlá M1 a N1. Problematike eCall zariadenia pre nákladné vozidlá sa venovali napríklad autori Oorni a kol. [21], kde analyzovali riešenia pre zisťovanie druhu prevážaného nákladu a dôležité informácie pre operačné strediská IZS.

Riešenie problematiky prepravy NL cestnou dopravou bolo súčasťou konzultácií s operačnými strediskami IZS. V prípade havárie nákladného vozidla s únikom NL boli identifikované nasledovné údaje, ktoré sú potrebné pre pracovníkov operačného strediska IZS a zasahujúce jednotky. Sú to:

- druh NL a jej klasifikácia,
- množstvo NL,
- preventívne a zmierňujúce opatrenia,
- spôsob nakladania a hasenia NL
- a pohotovostné číslo [23].

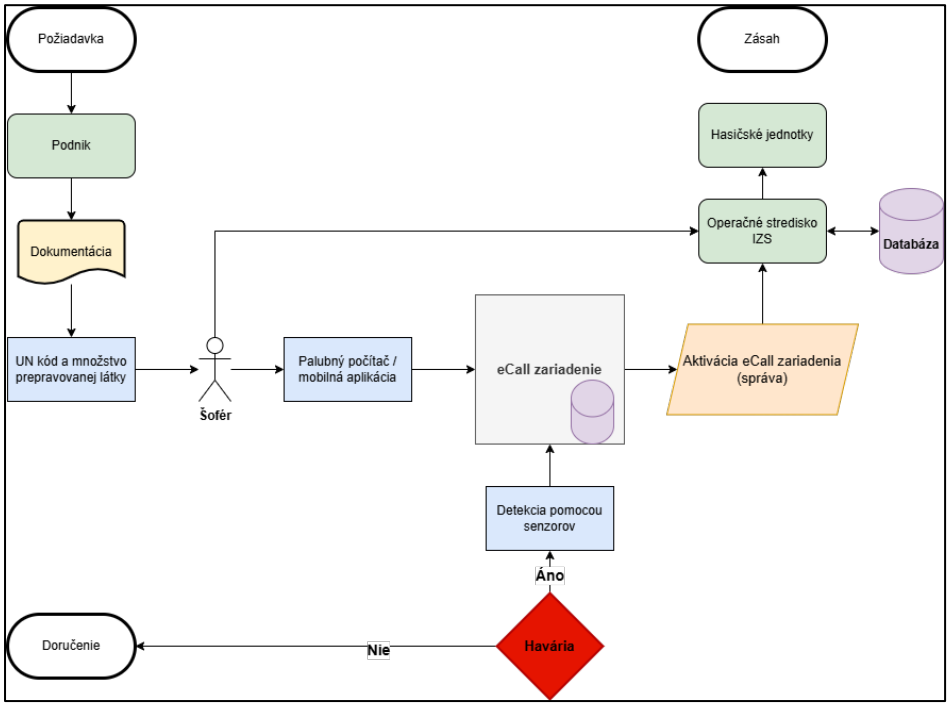
Poznanie daných informácií umožňuje vykonať prvotný zásah na obmedzenie úniku NL a správne zaobchádzanie s nimi. Informácie o druhu látky a jej klasifikácie, umožní nasadiť vhodné ochranné prostriedky a pristúpiť k opatreniam na ochranu života a zdravia. Zasahujúce jednotky teda okrem tzv. H-viet, ktoré sú súčasťou premenných uvedených v tabuľke 1, potrebujú aj tzv. P-vety. P-vety navádzajú na opatrenia, ktoré by mali byť prijaté pri manipulácií s danou látkou. Množstvo látky, ktoré je potrebné zadať v softvérovom nástroji pre potrebu výpočtu rozsahu úniku, ďalej slúži na stanovenie množstva

sorpčných prostriedkov. Pohotovostné číslo je dôležité, pre kontaktovanie osoby, ktorá bude zodpovedná za prečerpávanie a odvoz zvyšku NL.

Aplikovaním pôvodného princípu eCall, v spojení s palubným počítačom alebo aplikáciou, môžeme doplniť vstupné údaje, ktoré budú zasielané operačným strediskám IZS v prípade dopravnej nehody. Navrhujeme dve možnosti:

1. Prepojenie palubného počítača s eCall, do ktorého bude nahrávané identifikačné číslo NL a jej množstvo.
2. Tvorba aplikácie prepojenej so zariadením eCall pomocou bluetooth.

Samotný proces fungovania navrhovaného riešenia je znázornený na obrázku 1, ktorý znázorňuje vzťahy a následnosť jednotlivých udalostí pri preprave NL.



Obrázok 1 Model eCall nákladného vozidla prepravujúceho nebezpečnú látku

Model znázorňuje podnik, ktorý poskytuje vstupnú informáciu vo forme dokumentácie o prepravovanej NL vodičovi. Následne by mal vodič zaznamenať UN kód a prevážané množstvo NL z týchto dokumentov do palubného počítača alebo do aplikácie v mobilnom telefóne. Tieto údaje sa následne ukladajú na pamäťový priestor eCall zariadenia. Zariadenie je prepojené so senzormi, ktoré slúžia na detekciu nehody. Ak k nehode dôjde, zariadenie eCall sa aktivuje a odosiela správu aj s dodatočnými údajmi. Zároveň nasleduje hlasový hovor medzi vozidlom a operačným strediskom IZS a vysielajú sa zásahové jednotky. Nakoľko operačné stredisko IZS už disponuje informáciou o NL a jej množstve, už počas výjazdu komunikuje so zasahujúcimi jednotkami.

V prípade vytvorených scenárov, na základe údajov uvedených v tabuľke 1, by po obdržaní správy z eCall zariadenia, mohol operačný pracovník priamo, alebo zaslaním informácie pracovníkovi krízového riadenia, okamžite preveriť predpokladaný rozsah a následky úniku identifikovanej NL. Keďže eCall zariadenie zašle údaje zo vzniknutej havárie v reálnom čase, je možné upraviť tento scenár podľa aktuálnej lokácie, množstva príslušnej NL a meteorologických podmienok. Údaje z eCall zariadenia budú tak využité nielen zasahujúcimi zložkami IZS ale i krízovým riadením pri rozhodovaní o opatreniach na ochranu osôb, zvierat a životného prostredia.

4 ZÁVER

Riešenie, ktorým sa zaoberá tento príspevok, podporuje aktuálny vývoj v oblastí technológií a konceptu internetu vecí. Aplikovanie eCall zariadenia pre nákladné vozidlá prevážajúce NL prináša niekoľko výhod. Základnou výhodou je okamžitá informácia o dopravnej nehode priamo na operačné stredisko IZS spolu s údajmi o prepravovanej NL a jej množstve. Aplikovaním a rozšírením eCall zariadenia pre prepravu NL je možné predpokladať zvýšenie bezpečnosti zasahujúcich jednotiek, nakoľko dôjde k skráteniu času identifikácie NL. Informácie o možnom nebezpečenstve, umožnia včasné prijatie adekvátnych opatrení. Navrhované riešenie je však potrebné podrobiť podrobnému skúmaniu a výberu vhodných technologických riešení.

V príspevku boli tiež identifikované a kategorizované základné premenné, ktoré nájdu svoje uplatnenie najmä v predkrízovej fáze v procese posudzovania rizík prepravy NL. Posúdenie rizika umožní identifikovať oblasti, ktoré sú z pohľadu možných následkov najzraniteľnejšie. Následné vytvorenie scenárov havárií však nájde uplatnenie v podpore rozhodovania počas reakcie a riešenia mimoriadnej udalosti. Preto je v ďalšom výskume potrebné venovať pozornosť integrácií potrebných údajov a ich využitiu pomocou GIS a aplikačných softvérov.

POĎAKOVANIE

Financované EÚ NextGenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu č. 09I03-03-V05-00002.

LITERATÚRA

[1] ŘEHÁK, D.; RADIMSKY, M.; HROMADA, M.; DVOŘÁK, Z. 2019. Dynamic Impact Modeling as a Road Transport Crisis Management Support Tool. In: Adm. Sci. 2019, 9(2), 29. Dostupné na internete: https://doi.org/10.3390/admsci9020029

[2] LOVEČEK, T.; ŠISER, A.; MARIŠ, L. 2017. Use case of waterwork physical protection system robustness evaluation as a part of Slovak critical infrastructure. In: International Carnahan Conference on Security

Technology, Madrid, Spain, 2017, pp. 1-5. Dostupné na internete: doi: 10.1109/CCST.2017.8167811
[3] PURSIAINEN, CH. 2017. *The crisis management cycle*. 1. vydanie. Abingdon: Routledge. 194 s. ISBN: 978-1-315-62917-9.
[4] ŘEHÁK, D.; PATRMAN, D.; BRABCOVÁ, V.; DVOŘÁK, Z. 2020. Identifying critical elements of road infrastructure using cascading impact assessment. In: Transport, 35(3), 300-314. Dostupné na internete: https://doi.org/10.3846/transport.2020.12414
[5] KUBÁS, J.; KOLLÁR, B.; RISTVEJ, J.; PETRLOVÁ, K.; BLAŽKOVÁ, K. 2024. Vulnerability Assessment of Transport Infrastructure Elements - Case Study in Rajec. In: *Communications - Scientific Letters of the University of Zilina*, *26*(4), F23-35. Dostupné na internete: doi: 10.26552/com.C.2024.040
[6] LIU, L.; WU, Q.; LI, S.; LI, Y.; FAN, T. 2021. Risk Assessment of Hazmat Road Transportation Considering Environmental Risk under Time-Varying Conditions. In: International Journal of Environmental Research and Public Health, 18, 9780. Dostupné na internete: https://doi.org/10.3390/ijerph18189780.
[7] MARKOVÁ, I.; KUBÁS, J.; BUGANOVÁ, K.; RISTVEJ, J. 2022. Usage of sorbents for diminishing the negative impact of substances leaking into the environment in car accidents. In: Frontiers in Public Health, Volume 10. Dostupné na internete: https://doi.org/10.3389/fpubh.2022.957090.
[8] Analýza možného vzniku mimoriadnej udalosti v územnom obvode Okresného úradu Žilina. 2024 [online]. Ministerstvo vnútra Slovenskej republiky- Okresný úrad Žilina [cit. 2025-03-31]. Dostupné na: https://www.minv.sk/?okresne-urady-klientske-centra&urad=28&odbor=4
[9] Analýza územia z hľadiska možných mimoriadnych udalostí v územnom obvode Okresného úradu Kysucké Nové Mesto. 2024 [online]. Ministerstvo vnútra Slovenskej republiky- Okresný úrad Kysucké Nové Mesto [cit. 2025-03-31]. Dostupné na: https://www.minv.sk/?Oznamy_a_informacie_by
[10] Analýza možného vzniku mimoriadnej udalosti v územnom obvode Okresného úradu Liptovský Mikuláš. 2024 [online]. Ministerstvo vnútra Slovenskej republiky- Okresný úrad Liptovský Mikuláš [cit. 2025-03-31]. Dostupné na: https://www.minv.sk/?okresne-urady-klientske-centra&urad=31&sekcia=dokumenty-na-stiahnutie#popis
[11] Analýza možného vzniku mimoriadnej udalosti v územnom obvode Okresného úradu Bratislava. 2025 [online]. Ministerstvo vnútra Slovenskej republiky- Okresný úrad Bratislava [cit. 2025-03-31]. Dostupné na: https://www.minv.sk/?okresne-urady-klientske-centra&urad=1&sekcia=dokumenty-na-stiahnutie#popis
[12] Odbory krízového riadenia na okresných úradoch v sídle kraja. 2025. *Konzultácie k spracovaniu a využitiu Analýzy územia z hľadiska vzniku možných mimoriadnych udalostí* [polo-štruktúrovaný rozhovor]. Informácie pre: Boris KOLLÁR. 2024-12-17 - 2025-1-29 [cit. 2025-03-31]. Osobná komunikácia.

[13] HUANG, X.; WANG, X.; PEI, J.; et al. 2018. Risk assessment of the areas along the highway due to hazardous material transportation accidents. In: *Natural Hazards*, 93, 1181–1202. Dostupné na internete: https://doi.org/10.1007/s11069-018-3346-4.
[14] KUBAS, J.; POLORECKA, M.; HOLLA, K.; SOLTES, V.; KELISEK, A.; STRACHOTA, S.; MALY, S. 2022. Use of Toxic Substance Release Modelling as a Tool for Prevention Planning in Border Areas. In: *Atmosphere*, 13, 836. Dostupné na internete: https://doi.org/10.3390/atmos13050836.
[15] RISTVEJ, J.; ONDREJKA, R.; JÁNOŠÍKOVÁ, M. 2018. *Crisis management II. - 2nd part: application software in crisis management*. 1st ed. Žilina: University of Žilina. 2018. 271 pp. ISBN 978-80-554-1508-6.
[16] MA, C.; HAO, W.; PAN, F.; XIANG, W. 2018. Road screening and distribution route multi-objective robust optimization for hazardous materials based on neural network and genetic algorithm. In: *PLOS ONE*, 13(6), e0198931. Dostupné na internete: https://doi.org/10.1371/journal.pone.0198931.
[17] STOLECKA, K. 2020. Hazards of the Road Transportation of Hazardous Materials. In: System Safety: Human - Technical Facility - Environment, 2(1), 237–246. Dostupné na internete: https://doi.org/10.2478/czoto-2020-0029.
[18] United Nations (Ed.), 2016. European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR)- Volume 1. United Nations, New York and Geneva.
[19] United Nations (Ed.), 2023. Globally harmonized system of classification and labelling of chemicals (GDG), Tenth revised edition. ed. United Nations, New York and Geneva.
[20] CABO, M.; FERNANDES, F.; PEREIRA, T.; FONSECA, B.; PAREDES, H. 2014. Universal Access to eCall System. In: *Procedia Computer Science*, Volume 27, 104–112. ISSN 1877-0509. Dostupné na internete: https://doi.org/10.1016/j.procs.2014.02.013.
[21] OORNI, R.; MARINIC, G.; BEEHAREE, A.; LINKE, H.; TROSH, M. 2021. eCall for Heavy Goods Vehicles. In: *IEEE Intelligent Transportation Systems Magazine*, 13(2), 166–176. Dostupné na internete: https://doi.org/10.1109/MITS.2019.2898971.
[22] BONYÁR, A.; et al. 2017. A review on current eCall systems for autonomous car accident detection. In: *2017 40th International Spring Seminar on Electronics Technology (ISSE)*, Sofia, Bulgaria, pp. 1–8. Dostupné na internete: https://doi.org/10.1109/ISSE.2017.8000985.
[23] Koordinačné stredisko integrovaného záchranného systému Žilina. 2024. *Využívanie a funkcionalita nástroja eCall* [polo-štruktúrovaný rozhovor]. Informácie pre: Daniel CHOVANEC. 2024-11-28 [cit. 2025-03-31]. Osobná komunikácia.

MIKROPLASTY V HASEBNÍCH VODÁCH

Lucie Králová[1], Karla Barčová[2], Petr, Adamus[3]

ABSTRAKT

Projekt se zabývá výskytem mikroplastů v hasebních vodách a jejich možné dopady na životní prostředí a lidské zdraví. Zaměřuje se na identifikaci mikroplastů, identifikaci zdrojů mikroplastového znečištění a možnosti jeho omezení. Důraz je kladen na efektivitu dekontaminačních a filtračních metod, s cílem snížit množství mikroplastů uvolňovaných do životního prostředí, například z kontaminovaných zásahových obleků. Výstupy projektu pomohou lépe pochopit problematiku mikroplastů v hasičské praxi a navrhnout opatření ke snížení jejich výskytu.

KĽÚČOVÉ SLOVÁ

mikroplasty, hasební vody, znečištění, dekontaminace, filtrace

ABSTRACT

The project examines the occurrence of microplastics in firefighting water and their potential impact on the environment and human health. It focuses on the identification of microplastics, the identification of sources of microplastic contamination, and possible ways to reduce it. Emphasis is placed on the effectiveness of decontamination and filtration methods to minimize the release of microplastics into the environment, for example, from contaminated firefighting suits. The project's findings will contribute to a better understanding of microplastic issues in firefighting practice and help develop measures to reduce their occurrence.

KEY WORDS

microplastics, firefighting water, contamination, decontamination, filtration

1 Lucie, Králová Ing., VŠB – TU Ostrava, Lumírova 630/13 700 30 Ostrava-Výškovice, kra0545@vsb.cz,
2 Karla, Barčová doc. RNDr. Ph.D., VŠB – TU Ostrava, Lumírova 630/13 700 30 Ostrava-Výškovice, karla.barcova@vsb.cz,
3 Petr, Adamus Ing., VŠB – TU Ostrava, Lumírova 630/13 700 30 Ostrava-Výškovice, petr.adamus.st@vsb.cz

1 MIKROPLASTY

Mikroplasty jsou drobné plastové částice menší než 5 mm. Částice mohou být mikroskopické (neviditelné pouhým okem) nebo viditelné jako drobné úlomky, které vznikají buď záměrně, nebo degradací větších plastových předmětů. Rozlišujeme primární a sekundární mikroplasty. Primární mikroplasty jsou vyráběny přímo v této velikosti, například pro použití v kosmetických přípravcích, čisticích prostředcích nebo v průmyslu. Sekundární mikroplasty se tvoří rozpadem větších plastů, jako jsou láhve, obaly, rybářské sítě, igelitové tašky, vlivem UV záření, mechanického opotřebení a jiných procesů [5,7].

Mikroplastické částice jsou chemicky stálé, těžko rozložitelné a zůstávají v přírodě po dlouhou dobu. Mikroplasty jsou vysoce odolné vůči biologickým i fyzikálním vlivům. Nacházejí se ve vodních ekosystémech, v půdě, na sedimentech i vzduchu, kde se hromadí a postupně vstupují do potravního řetězce. Mikroplasty také absorbují toxické látky, jako jsou pesticidy, těžké kovy a další znečišťující látky, což zvyšuje jejich škodlivý potenciál pro organismy, včetně člověka. Jejich přítomnost v prostředí je považována za závažný ekologický problém, který vyžaduje důsledné řešení a omezení používání plastů [2,3,5].

1.1 POZITIVNÍ ÚČINKY

I když jsou mikroplasty vnímány především jako environmentální problém, mohou mít v určitých kontextech pozitivní využití díky svým vlastnostem. Mikroplasty, stejně jako nanočástice bývají využity jako nosiče léků v medicíně. Pomáhají přesně dopravit léčiva na místo určení v těle. Dále se používají v moderních technologiích, například při vývoji filtračních materiálů nebo lehkých kompozitů. Mikroplasty z recyklovaných plastů mohou být využity pro výrobu nových produktů, čímž se snižuje celková potřeba těžby nových surovin. Uplatnění nacházejí mikroplasty například v technologii 3D tisku. Dále zlepšují vlastnosti výrobků, jako je pružnost nebo odolnost [1,8].

1.2 NEGATIVNÍ ÚČINKY

Mikroplasty mají řadu negativních důsledků, které ovlivňují životní prostředí, zdraví organismů i lidskou populaci. Jedním z hlavních problémů je jejich dlouhá životnost a nerozložitelnost, díky čemuž se hromadí v přírodě, zejména ve vodních ekosystémech, půdě a vzduchu. Tyto drobné plastové částice se dostávají do potravního řetězce, protože je nechtěně konzumují živočichové, zejména mořské organismy, jako jsou ryby, korýši nebo ptáci. To způsobuje fyzické problémy, například záněty, blokaci trávicího traktu nebo úhyn zvíře [4,5,7].

Mikroplasty slouží jako nosiče toxických látek, kdy tyto látky mohou při konzumaci pronikat do těla živočichů i lidí, což vede k potenciálním zdravotním

problémům, například k hormonálním poruchám, zánětům, či dokonce ke zvýšenému riziku vzniku rakoviny [4,5].

Dalším problémem je jejich přítomnost ve vzduchu, kde se šíří v podobě prachových částic. Při vdechování mohou mikroplasty negativně ovlivnit dýchací systém, vyvolávat alergie nebo chronické onemocnění plic. Mikroplasty se také nacházejí v pitné vodě a potravinách, což zvyšuje jejich expozici lidské populaci [4,5].

Ekologický dopad mikroplastů je závažný. Částice znečišťují prostředí, snižují kvalitu půdy a vody a negativně ovlivňují biodiverzitu. Postupně pronikají do nejodlehlejších oblastí světa, včetně polárních oblastí nebo hlubokých oceánů, což ztěžuje jejich odstranění a kontrolu. Problematika mikroplastů proto představuje globální výzvu, která vyžaduje snížení produkce plastového odpadu, podporu recyklace a vývoj alternativních materiálů šetrných k životnímu prostředí [4,5].

2 MIKROPLASTY V KAPALINÁCH

Mikroplasty ve vodách představují vážný environmentální problém, který zasahuje vodní ekosystémy i kvalitu pitné vody a přírodní vody. Tyto drobné plastové částice se dostávají do vodních prostředí především z odpadních vod, kde pocházejí z různých zdrojů a procesů. Jak již bylo zmíněno, mikroplasty jsou vysoce odolné vůči rozkladu, což jim umožňuje dlouhodobě přetrvávat ve vodě, kde se šíří díky proudům i na velké vzdálenosti, včetně nejodlehlejších oblastí, jako jsou hluboké oceány nebo polární moře. Tyto částice se vznášejí na hladině, usazují se na dně nebo zůstávají suspendované ve vodním sloupci. Vodní organismy, například plankton, ryby nebo korýši, je často zaměňují za potravu, což vede k jejich bioakumulaci v potravním řetězci. Konzumace mikroplastů může způsobit fyzické blokace trávicího traktu, záněty a další zdravotní problémy u živočichů [4,5,6,7].

2.1 MIKROPLASTY V PITNÉ VODĚ

Kromě ekologických dopadů byly mikroplasty experimentálně zjištěny v pitné vodě, a to jak v balené, tak v kohoutkové. Tyto částice se do pitné vody dostávají z nedostatečně čištěných odpadních vod, rozpadu plastových potrubí nebo atmosférického znečištění. I když zdravotní rizika spojená s mikroplasty pro člověka zatím nejsou zcela prozkoumána, existují obavy, že jejich konzumace může způsobit záněty, hormonální poruchy nebo ovlivnit imunitní systém. Mikroplasty ve vodách jsou obtížně odstranitelné, protože jejich malá velikost často uniká tradičním filtračním procesům v čistírnách odpadních vod. Řešení tohoto problému zahrnuje snižování produkce plastového odpadu, zlepšení filtračních technologií a podporu biologicky odbouratelných materiálů, které by mohly nahradit konvenční plasty [3,5,6].

2.2 MIKROPLASTY V HASEBNÍCH VODÁCH

Mikroplasty v hasebních vodách představují méně známý, avšak významný problém, který se týká nejen ochrany životního prostředí, ale i zdraví lidí. Hasební vody vznikají při hašení požárů, zejména v průmyslových oblastech, a často obsahují směsi chemikálií, zplodin hoření a dalších nečistot, mezi nimiž mohou být i mikroplasty. Tyto plastové částice se do hasebních vod dostávají rozpadem plastových materiálů během požárů, uvolňováním z hasicích přístrojů nebo jako součást pěnových hasiv používaných při zásazích.

Během hašení požárů plastů, automobilů nebo budov, které obsahují velké množství syntetických materiálů, dochází k jejich tepelnému rozkladu. Některé plasty se úplně nespálí a fragmentují se na mikročástice, které se následně splavují hasební vodou. Tyto vody, pokud nejsou správně zachyceny a vyčištěny, mohou pronikat do povrchových vod, půdy nebo podzemních vod, čímž přispívají ke kontaminaci prostředí [4,5,6,7].

V hasebních vodách mají mikroplasty podobné negativní důsledky jako mikroplasty v jiných vodních prostředích. Mohou se šířit v ekosystémech, být konzumovány vodními organismy a dále se bioakumulovat v potravním řetězci. Řešením tohoto problému je především důsledná kontrola a záchyt hasebních vod při požárních zásazích, zejména v průmyslových oblastech, kde je vysoké riziko znečištění plastovými materiály. Je důležité používat moderní technologie na čištění hasebních vod a minimalizovat použití plastů ve stavebnictví a průmyslu, aby se snížil potenciální vznik mikroplastů během požárů. Významnou roli hraje také výzkum zaměřený na nahrazení běžných hasiv biologicky odbouratelnými alternativami, které by nezvyšovaly zátěž na životní prostředí [4,5,6,7].

3 FYZIKÁLNÍ PRINCIPY MĚŘENÍ

Pro provedení experimentální části práce bude použito několik mikroskopických metod.

3.1 METODA SEM

Metoda SEM patří pod elektronovou mikroskopii a jde o skenovací neboli rastrovací/řádkovací elektronový mikroskop. Jedná se o optický přístroj. Obraz je vytvořen pomocí elektromagnetických čoček a zdroje záření - elektronů. Pomocí metody SEM lze pozorovat povrch detekovaných objektů, dále lze zjistit jejich velikost, informace o mikrostruktuře, o krystalografickém uspořádání či o chemickém složení [1].

3.2 METODA TEM

Transmisní elektronová mikroskopie, což vysvětluje zkratku z angličtiny TEM, se řadí mezi analytické metody, konkrétně také elektronovou mikroskopii a nejvíce se přibližuje mikroskopii světelné. Při použití metody TEM dojde k prosvícení celého vzorku najednou pomocí elektronového svazku vycházejícího ze zdroje [1].

3.3 METODA STEM

Spojením metod SEM a TEM vzniká metoda STEM, neboli skenovací transmisní elektronová mikroskopie. Obraz vzniká skenováním fokusovaným svazkem na vzorku, který musí být kompatibilní pro elektrony a detekcí prošlých elektronů. Metodou se dají detekovat jednotlivé atomy ve vzorku a také lze mapovat chemické složení vzorku za využití dalších pomocných metod [1].

3.4 METODA AFM

Mikroskopie atomárních sil, AFM, je metoda, kterou řadíme mezi mikroskopii skenující sondou. Jedná se o metodu, při níž dochází k měření meziatomárních sil a obraz se získává při přiblížení sondy/hrotu k povrchu vzorku [1].

3.5 METODA HRTEM

Metoda HRTEM, což v překladu znamená transmisní elektronová mikroskopie s vysokým rozlišením, vychází z metody HREM (= Elektronová mikroskopie s vysokým rozlišením), ve které jsou obrazy tvořeny atomovou mřížkou [1].

3.6 OPTICKÝ MIKROSKOP

Optická mikroskopie, jinak řečeno světelná mikroskopie, je jedna z dalších možných zobrazovacích metod s širokým uplatněním v praxi. Rozsáhlé uplatnění v praxi lze přikládat pro značnou nenáročnost na přístroje, vybavení a snadné ovládání. Metodou lze zobrazit a zvětšit různé materiály/vzorky, rozeznat rozdílné struktury, mikroskop dokáže zobrazit pohyb částic v kapalině [1].

4 POSTUP ŘEŠENÍ

Pro naplnění cílů bude provedena důkladná rešerše aktuálního stavu poznání a obdobných experimentálních prací, které by mohly vznést důležité informace pro směřování projektu.

Bude provedeno kontaktování laboratoří a pracovišť, disponující jednotlivými mikroskopy pro identifikaci, detekci mikroplastů a jejich následnou analýzu z hasebních vod. Dále dojde k zajištění potřebného materiálu pro odebrání vzorků, popis vzorků, uchování vzorků, specifický materiál potřebný pro provedení analýzy u jednotlivých mikroskopů. Jakmile budou laboratoře dostupné a zajištěn materiál, proběhne odebrání vzorků z různých stanic Hasičského záchranného sboru ČR, ať už od dobrovolných nebo profesionálních. Vzorky budou odebrány z míst při plnění cisteren vodou, z různých cisteren. Voda bude jinou časovou dobu uchována v cisternách, voda bude odebrána z různých vodních zdrojů.

V rámci projektu se předpokládá spolupráce s Univerzitou Palackého v Olomouci, se kterou byla již v minulosti navázána spolupráce při řešení obdobných projektů. V rámci projektu poskytnou zařízení HRTEM, včetně odborné obsluhy.

V dalším kroku proběhne jedna z hlavních částí experimentálního měření, kdy bude z každého vzorku experimentálně zjištěno množství mikroplastů, velikost a chování mikroplastů, charakteristika vzorků a tak dále. Další hlavní částí experimentu bude návrh řešení na eliminaci a zadržení mikroplastů při používání vody z cisteren při záchranných a likvidačních prací hasičských záchranných sborů. Předmětem výzkumu a jednou z možných alternativ bude použití mechanických filtrů, aktivního uhlí, adsorpčních materiálů, biologických filtrů a jiné.

Další dílčí experimentální částí práce bude ověření přítomnosti mikroplastů na ochranných oděvech jednotek požární ochrany po ukončení zásahu. Tento postup bude zahrnovat testování „znečištěného“ oděvu po zásahu a následnou analýzu po jeho vyprání, čímž dojde k vyhodnocení účinnosti běžných čistících metod při eliminaci mikroplastů z ochranných oděvů.

Výsledkem experimentu bude navrhnout optimalizovaný odběr vzorků z hasebních vod, proces laboratorní předúpravy, způsob analytického monitoringu a zejména eliminaci a zadržení mikroplastů, z důvodu zredukovat riziko znečištění životního prostředí, objektů i předmětů zásahu a snížit vdechování mikroplastů při zásahu hasičů a používání vody z cisteren.

5 PŘÍNOSY

Návrh experimentu odpovídá zaměření Katedry požární ochrany a Katedry bezpečnostních služeb, Fakulty bezpečnostního inženýrství Vysoké školy báňské – Technické univerzity Ostrava. Výsledky experimentu budou sloužit k dopracování disertační práce, a to na téma „Mikroplasty v hasebních vodách“. Výsledky projektu budou přínosem pro vědní obor a rozšiřování povědomí o mikroplastech ve vodách v České republice. V současnosti je problematika mikroplastů ve vodách v českém prostředí silně opomíjená, ač mikroplasty ve vodních systémech v zahraničí získávaji stále větší popularitu pro výzkum. Každým rokem probíhá v zahraničí nespočet experimentálních prací, které se zabývají právě výskytem mikroplastů v pitné vodě, ale zejména v přírodních tocích a také přehledem jejich dopadů na životní prostředí a jejich potenciálním rizikem. Momentálně neexistuje práce, která by se komplexně zabývala mikroplasty v hasebních vodách a účinky na životní prostředí, na zasahující hasiče používajících hasební vodu při zásazích. Výsledky projektu by měly vést k žádoucímu nárůstu testování mikroplastů ve vodách v českém prostředí a implementaci experimentálních poznatků do dalších prací, jelikož tyto poznatky mohou být pro životní prostředí a průmysl zásadní.

LITERATÚRA

[1] KRÁLOVÁ, Lucie. Zhodnocení možností mikroskopické detekce nanočástic. Online, Diplomová práce. Ostrava: Vysoká škola báňská – Technická univerzita Ostrava, 2024. Dostupné z: http://hdl.handle.net/10084/153483. [cit. 2025-04-02].

[2] ERMOLIN, Michail. Assessment of the Microplastics Content in Natural Waters and Sediments: Sampling and Sample Preparation. Online. JOURNAL OF ANALYTICAL CHEMISTRY. 2024, s. 19. Dostupné z: https://doi.org/10.1134/S1061934824050058. [cit. 2024-12-19].

[3] JANG, Ling; KANG, Shichang a LUO, Si. Microplastics in drinking water: A review on methods, occurrence, sources, and potential risks assessment. Online. *ENVIRONMENTAL POLLUTION*. 2024. Dostupné z: https://doi.org/10.1016/j.envpol.2024.123857. [cit. 2024-12-19].

[4] CHANDRA, Shaneel a WALSH, Kerry. Microplastics in water: Occurrence, fate and removal. Online. *JOURNAL OF CONTAMINANT HYDROLOGY*. 2024. Dostupné z: https://doi.org/10.1016/j.jconhyd.2024.104360. [cit. 2024-12-19].

[5] KYE, Honim; KIM, Ťi-jüon a JU, Seonghyeon. Microplastics in water systems: A review of their impacts on the environment and their potential hazards. Online. *HELIYON*. 2024. Dostupné z: https://doi.org/10.1016/j.heliyon.2023.e14359. [cit. 2024-12-19].

[6] TANG, Shuyuan; GAO, Ling a TIAN, Aisi. The coagulation behavior and removal efficiency of Mikroplasty in drinking water treatment. Online. *JOURNAL OF WATER PROCESS ENGINEERING*. 2023. Dostupné z: https://doi.org/10.1016/j.jwpe.2023.103885. [cit. 2024-12-19].

[7] ZOPPAS, Fernanda Miranda; SACCO, Nicolas a SOFFIETTI, Jesica. Catalytic approaches for the removal of microplastics from water: Recent advances and future opportunities. Online. *CHEMICAL ENGINEERING JOURNAL ADVANCES*. 2023. Dostupné z: https://doi.org/10.1016/j.ceja.2023.100529. [cit. 2024-12-19].
[8] CAO, Ngoc-Dan-Thanh; VO, Dieu-Hien Thi a PHAM, Mai-Duy-Thong. Microplastics contamination in water supply system and treatment processes. Online. *SCIENCE OF THE TOTAL ENVIRONMENT*. 2024. Dostupné z: https://doi.org/10.1016/j.scitotenv.2024.171793. [cit. 2024-12-19].

APLIKÁCIA KORELAČNEJ ANALÝZY NA STAVEBNOTECHNICKÝ STAV MOSTOV NA SLOVENSKU

Michal Miške[1]

ABSTRAKT

Cieľom tohto článku je preskúmať vzťah medzi stavebnotechnickým stavom mostov a rokom ich výstavby. Po akvizícii dát o mostoch z rôznych časových období bol vyhodnotení súčasný stavebnotechnický stav v závislosti od roku skonštruovania mostného objektu. Prostredníctvom korelačnej analýzy bola pozorovaná závislosť medzi rokom výstavby a stavebnotechnickým stavom mostov, pričom základný predpoklad znie, že staršie mosty by mali byť alebo majú tendenciu byť v horšom stave. Korelačný koeficient však ukázal, že táto závislosť je slabá. Záverom tejto analýzy je teda tvrdenie, že rok výstavby nie je hlavným faktorom ovplyvňujúcim stavebnotechnický stav mostov. V budúcnosti by výskum mal zahŕňať ďalšie premenné, ako sú údržba, materiály a zaťažiteľnosť.

Kľúčové slová:
Most, Stavebnotechnický stav, Cesty, Kritická infraštruktúra.

ABSTRACT

The aim of this paper is to investigate the relationship between the structural-technical condition of bridges and the year of their construction. After acquiring data on bridges from different time periods, the current structural engineering condition was evaluated in relation to the year of construction of the bridge structure. Through correlation analysis, a dependency between the year of construction and the structural-technical condition of the bridges was observed, with the basic assumption being that older bridges should be or tend to be in worse condition. However, the correlation coefficient showed that this dependence is weak. Thus, the conclusion of this analysis is that the year of construction is not a major factor influencing the structural condition of bridges. Future research should include other variables such as maintenance, materials and load capacity.

Key words:
Bridge, Structural Health, Roads, Critical Infrastructure.

1 Michal Miške, Ing. Žilinská univerzita v Žiline, Fakulta bezpečnostního inžinierstva, mail: michla.miske@uniza.sk

1 ÚVOD DO PROBLEMATIKY

Príspevok sa zameriava na štatistický prieskum mostov na cestách prvej triedy na Slovensku. Na Slovensku sa cestná sieť skladá z rôznych typov ciest a klasifikácií, ktoré odrážajú ich význam či špecifickú funkciu v rámci dopravného systému. Podľa dopravného významu sa slovenské cesty členia na diaľnice, cesty prvej triedy, cesty druhej triedy, cesty tretej triedy a miestne komunikácie v súvislosti so zákonom 135/1961 Z. z. o pozemných komunikáciách [1]. Každý typ má špecifické vlastnosti, ako sú šírka, kvalita povrchu, intenzita dopravy, druh a frekvencia dopravných stavieb. Na cestných komunikáciách sa nachádzajú rôzne stavby, ktoré umožňujú prekonávanie prírodných a umelých prekážok, čím sa zabezpečuje plynulosť dopravnej infraštruktúry. Každý typ cesty spravujú rôzne subjekty, ktoré môžu ovplyvniť súčasný stavebnotechnický stav týchto objektov (pozri tabuľku 1).

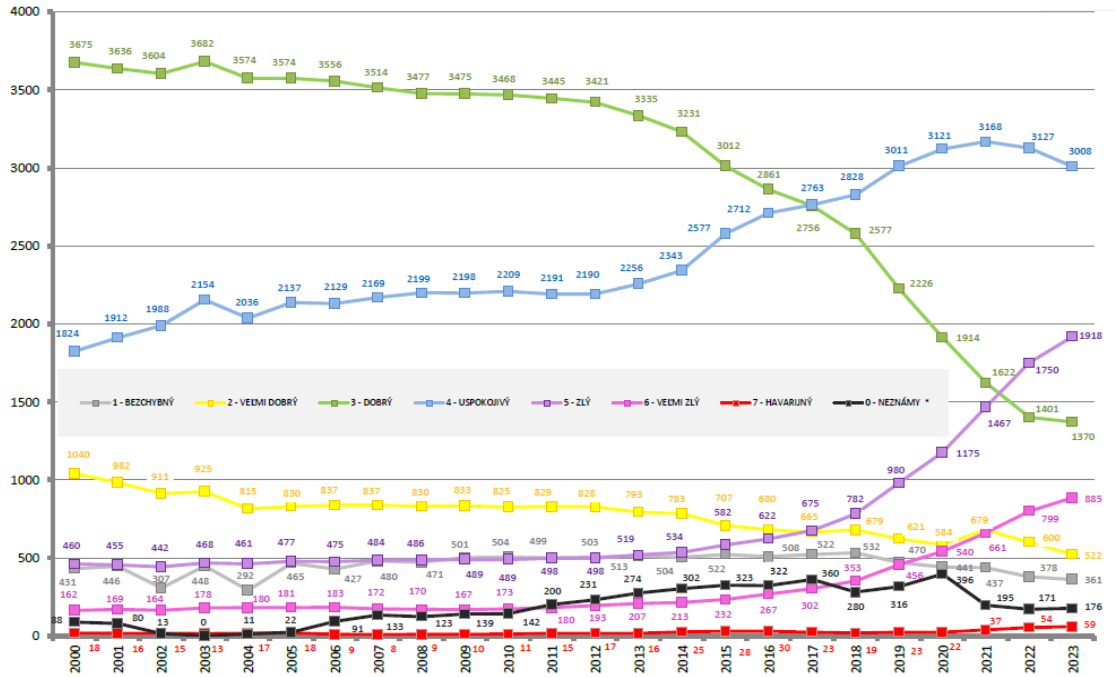
Tabuľka 1 Správcovia ciest a mostov na Slovensku

Druh cesty	Vlastník	Administrátor
Diaľnica	Štát	Národná diaľničná spoločnosť
Rýchlostné cesty		
Cesty I. II. III. triedy	Samosprávne kraje	Slovenská správa ciest
Miestne cesty	Obecné úrady	Obecné úrady

Neoddeliteľnou súčasťou cestnej siete sú tunely, križovatky, podchody a mosty. Mosty zohrávajú kľúčovú úlohu pri zabezpečovaní plynulosti a efektívnosti dopravy. Na Slovensku sa nachádza viac ako 8 000 mostov na všetkých typoch ciest. Tieto mosty sa líšia nielen veľkosťou a konštrukčným riešením, ale aj technickým stavom a nosnosťou. Na Slovensku sa už dlhé roky používajú rôzne typy predpätých nosníkov a po rokoch prevádzky je možné evidovať aj počty porúch na týchto prefabrikovaných predpätých nosníkoch či iných mostoch [2, 3]. Mosty, ktoré sú súčasťou ciest prvej triedy, majú často strategický význam, pretože slúžia ako hlavné dopravné tepny spájajúce veľké mestá, priemyselné oblasti a regionálne centrá. Ich technický stav, kapacita a bezpečnosť sú teda kľúčovými faktormi ovplyvňujúcimi kvalitu cestnej dopravy na Slovensku. Ďalším dôležitým faktorom stavebnotechnického stavu mosta môže byť vlastník a zodpovedné osoby konkrétneho mosta, pretože na Slovensku je veľa rôznych vlastníkov a zodpovedných osôb s rôznym prístupom k stavu mosta. Najdôležitejším aspektom z hľadiska bezpečnosti mostov je podľa Technických podmienok [4] práve úroveň stavebnotechnického stavu. Je reprezentovaná číslom od 1 do 7 (kde 1 je veľmi dobrý stav a 7 je havarijný stav), ktoré predstavuje komplexné hodnotenie mosta určené váženým priemerom jednotlivých hodnotení mostných objektov, resp. jednoduchým aritmetickým priemerom jednotlivých hodnotení mostných prvkov. Numericky opisuje technické a konštrukčné podmienky stavby. Mosty sa

kategorizujú do jednotlivých úrovní stavu na základe výsledkov pravidelných prehliadok [5, 6]. ktoré sa vykonávajú spravidla vizuálnou kontrolou, ale v poslednom období sa vo svete uplatňujú nové trendy ako kontrola pomocou rôznych typov bezpilotných lietadiel a robotov [7-10].

Za posledných 20 rokov sa výrazne zhoršil stavebnotechnický stav našich mostov, ako je znázornené na obrázku 1. Výrazný pokles, ako je možné vidieť, je v dobrom stave, kde za obdobie 23 rokov (od roku 2000 do roku 2023) zmenilo stavebnotechnický stav 3 675 mostov a súčasný počet je 1 370 mostov (úroveň 3, zelená čiara). Naopak, dramaticky vzrástol počet mostov v zlom stave (úroveň 5, fialová čiara) a veľmi zlom stave (úroveň 6, ružová čiara). Prírastok predstavuje hodnoty 460 až 1 918 v zlom stave a hodnoty 162 až 825 vo veľmi zlom stave.



Obrázok 2 Vývojový graf stavu mostov na Slovensku

Hlavným cieľom tohto prieskumu je analyzovať súvislosť medzi stavebnotechnickým stavom mostov a rokom ich výstavby. Štatistické údaje pochádzajú z Cestnej databanky (CDB) Slovenskej republiky (2024) [11]. Oddelenie CDB má na starosti centrálnu technickú evidenciu ciest, navrhovanie a posudzovanie trás pre prepravu nadrozmerných nákladov, ako aj prevádzku Dispečerského centra centrálnej spravodajskej služby (integrovaný informačný systém pre zimnú údržbu). Stavebnotechnický stav mostov úzko súvisí s ich odolnosťou resp. bezpečnosťou. Ak je most zaradený medzi prvky kritickej infraštruktúry, hovoríme konkrétne o odolnosti kritickej infraštruktúry. Touto problematikou sa zaoberajú Řehák a kol. [12] v rámci Metodiky hodnotenia odolnosti prvkov kritickej infraštruktúry (CIERA). Odolnosť sa pritom chápe ako vnútorná pripravenosť (kritických) infraštruktúrnych subsystémov na mimoriadne a neželané udalosti. Inými slovami, ide o schopnosť týchto systémov udržať svoju funkčnosť aj napriek nepriaznivým vonkajším alebo vnútorným vplyvom [13, 14].

2 APLIKÁCIA KORELAČNEJ ANALÝZY

V tejto časti sa podrobne analyzuje využitie korelačnej analýzy s cieľom porozumieť vzťahu medzi stavebnotechnickým stavom mostných objektov, ktoré sa nachádzajú **len na cestách I. triedy**, a rokom ich skonštruovania resp. výstavby. Cesty I. triedy sú štátne cesty s nadregionálnym dopravným významom, ktoré prepájajú dopravné uzly vyššej úrovne a napájajú ich na diaľnice [1]. Most predstavuje miesto križovania cesty s inou komunikáciou alebo s prírodnou či človekom vytvorenou prekážkou. Mosty sa ďalej členia na jednotlivé dilatačné celky, ktoré predstavujú najmenšiu evidenčnú jednotku mosta. Hlavným cieľom bolo zistiť, či existuje závislosť medzi týmito dvoma premennými, čo by mohlo naznačovať, že vek mosta zohráva významnú úlohu pri určovaní jeho aktuálneho stavebno-technického stavu. Analýzou tohto vzťahu sa snažíme identifikovať potenciálne vzorce, ktoré by mohli napomôcť pri tvorbe efektívnych stratégií údržby a pri plánovaní budúcich výstavieb. Na dosiahnutie tohto cieľa bol vypočítaný korelačný koeficient. Tento štatistický ukazovateľ poskytuje informácie o sile a smere lineárneho vzťahu medzi rokom výstavby a stavebno-technickým stavom mostov. Kladná korelácia by naznačovala, že s pribúdajúcim rokom výstavby sa stav mostov zlepšuje, zatiaľ čo záporná korelácia by znamenala opak. Výsledky analýzy ukázali, že hodnota korelačného koeficientu bola záporná, konkrétne -0,287, čo vyplýva z nasledujúceho vzorca [15]:

$$r = \frac{\sum x_i y_i - n * \bar{x} * \bar{y}}{\sqrt{(\sum x_i^2 - n * x^2) * \sum y_i^2 - n * y^2)}}$$

Po zakomponovaní všetkých mostných objektov ich stavebno-technického stavu a roku postavenia je výsledkom, vypočítaným cez excelovskú funkciu, korelačného koeficientu hodnota **-0,287**. Tento výsledok naznačuje slabú negatívnu koreláciu, ako je uvedené v tabuľke 2, čo naznačuje, že vo všeobecnosti majú staršie mosty tendenciu mať horší stavebno-technický stav v porovnaní s novšími. Korelácia však nie je silná, čo naznačuje, že hoci rok výstavby môže mať vplyv na stav mostov[16], môžu ich súčasný stav významne ovplyvniť aj iné faktory, ako napríklad údržba, použité materiály, podmienky prostredia a kvalita konštrukcie.

Tabuľka 2 Úroveň závislosti dvoch číselných znakov

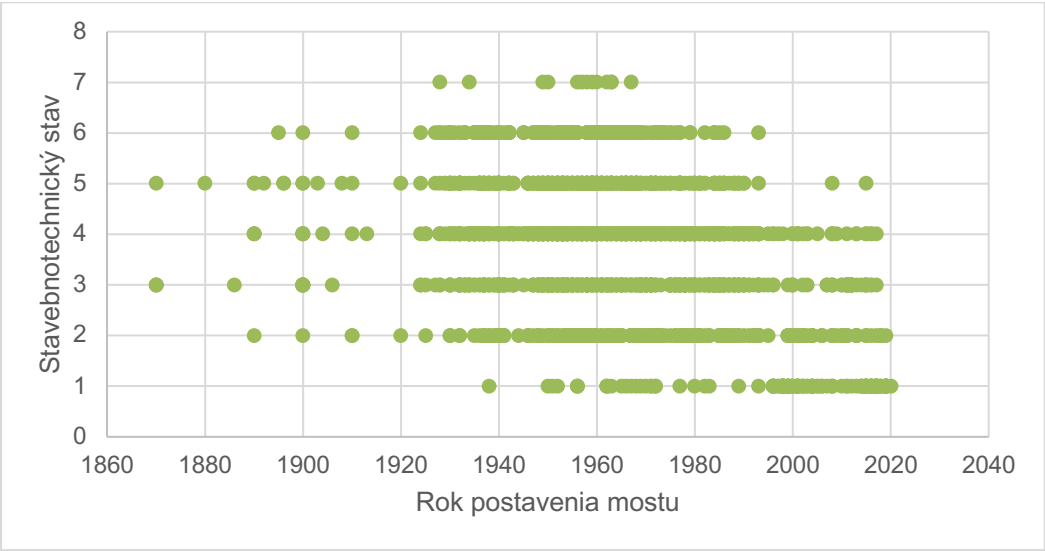
Úroveň závislosti	
Numericky	Slovne
<0; 0,2)	Veľmi slabá závislosť
<0,2; 0,4)	Slabá závislosť
<0,4; 0,6)	Stredná závislosť
<0,6; 0,8)	Silná závislosť
<0,8; 1>	Veľmi silná závislosť

Korelačný koeficient vyjadruje silu a smer vzťahu medzi dvoma premennými. Hodnoty korelačného koeficientu sa hýbu v rozmedzí od -1 do 1:

- +1 znamená dokonalú pozitívnu koreláciu (keď sa zvyšuje jedna premenná, zvyšuje sa aj druhá premenná),
- -1 znamená dokonalú negatívnu koreláciu (Keď jedna premenná klesá, druhá premenná rastie),
- 0 znamená, že medzi premennými neexistuje lineárna korelácia.

Záporná korelácia zistená v tejto analýze zdôrazňuje význam pravidelnej kontroly a údržby, najmä v prípade starších mostných konštrukcií. Zdôrazňuje potrebu cielených zásahov na odstránenie potenciálnych nedostatkov starších mostov, čím sa zabezpečí ich bezpečnosť a funkčnosť v priebehu času. Táto analýza poskytuje základ pre ďalší výskum, do ktorého možno zahrnúť viac premenných, aby sa lepšie pochopila komplexná dynamika ovplyvňujúca stav mosta. Budúce štúdie by mali zahŕňať faktory, ako je dopravné zaťaženie, geografická poloha, vplyv prostredia a historické záznamy o údržbe, aby sa vytvorilo komplexnejšie hodnotenie faktorov ovplyvňujúcich životnosť a bezpečnosť mostov. Záporný korelačný koeficient teda naznačuje, že s nárastom jednej premennej sa druhá znižuje, alebo v tomto prípade neskôr postavený most býva vo veľmi dobrom konštrukčnom stave. Rok výstavby je vyšší, znamená, že je novší, potom je konštrukčný stav skôr nižší (číslo 1 alebo 2). Nasledujúci obrázok 2 znázorňuje mosty na cestách 1. triedy na Slovensku podľa roku výstavby a stavebnotechnických podmienok.

Výsledky korelačnej analýzy ukazujú, že medzi týmito dvoma číselnými znakmi existuje len slabá závislosť. Je možné teda tvrdiť, že rok výstavby, v ktorom bol most postavený, nie je hlavným faktorom ovplyvňujúci zlý stavu mostného objektu.



Obrázok 3 Zobrazenie Stavebnotechnického stavu mostov a roku postavenia

3 DISKUSIA

Množstvo inžinierskych stavieb na Slovensku je dané predovšetkým rozmanitou a zložitou členitosťou krajiny, ktorá zahŕňa množstvo vodných tokov, riek, hôr a iných prírodných prekážok. Táto geografická rozmanitosť si vyžaduje rozvoj rozsiahlych infraštruktúrnych sietí vrátane ciest, mostov a informačných komunikačných sietí, aby sa zabezpečilo prepojenie a funkčnosť v rôznych regiónoch. Vzhľadom na tento kontext je nevyhnutné identifikovať hlavné faktory, ktoré negatívne ovplyvňujú stav týchto inžinierskych stavieb. Jedným z potenciálnych prispievateľov sú environmentálne podmienky v okolí objektov, napríklad vystavenie extrémnemu počasiu, kolísanie teplôt a prírodné katastrofy, ako sú záplavy alebo zosuvy pôdy, ktoré môžu časom urýchliť opotrebovanie a degradáciu stavu. Na druhej strane existujú značné obavy týkajúce sa prideľovania a riadenia finančných zdrojov v tomto sektore. Neefektívne investičné stratégie, nedostatočné financovanie pravidelnej údržby a oneskorené opravy môžu ešte viac zhoršiť funkčnosť štrukturálnej integrity. Riešenie týchto finančných problémov je nevyhnutné na predĺženie životnosti a zaistenie bezpečnosti týchto konštrukcií [17, 18]. V minulosti sa preferovalo, že proaktívne opatrenia, ako sú bežné kontroly a preventívna údržba, sú nákladovo efektívnejšie ako reaktívne opatrenia na poruchy konštrukcií alebo mimoriadne udalosti. Preventívne stratégie pomáhajú včas odhaliť potenciálne problémy, znižujú potrebu nákladných havarijných opráv a zmierňujú riziká pre verejnú bezpečnosť. Takýto prístup nielen šetrí finančné zdroje, ale podporuje aj dlhodobú odolnosť a bezpečnosť infraštruktúry, čím sa zabezpečuje, že dokáže účinnejšie odolávať tlakom prostredia a používania. V budúcnosti je nevyhnutné prijať vyváženejšiu stratégiu, ktorá kombinuje environmentálne riadenie s lepším finančným plánovaním a investíciami do preventívnej údržby. Riešením prírodných aj človekom spôsobených mimoriadnych udalostí môže Slovensko zvýšiť odolnosť a funkčnosť svojich inžinierskych stavieb, podporiť udržateľný rozvoj a zabezpečiť bezpečnosť a blahobyt svojich obyvateľov.

4 ZÁVER

Tento článok bol zameraný na korelačnú analýzu závislosti medzi rokom výstavby mostov na cestách I. triedy na Slovensku a ich súčasným stavebnotechnickým stavom. Korelačnou analýzou sme zistili slabú negatívnu závislosť medzi týmito premennými, čo naznačuje, že staršie mosty bývajú v horšom stave. Tento vzťah však nie je dostatočne silný na to, aby sme ho mohli považovať za rozhodujúci faktor ovplyvňujúci stavebnotechnický stav mostov. Na základe výsledkov je vhodné rozšíriť výskum o ďalšie premenné, ako sú údržba, použité materiály, zaťaženie a geografické podmienky, aby sme získali komplexnejšie poznatky o faktoroch ovplyvňujúcich stav mostov. Tento výskum by mohol poskytnúť cenné poznatky pre efektívnejšie plánovanie údržby a navrhovanie nových mostov, ktoré lepšie odolávajú mimoriadnym udalostiam.

POĎAKOVANIE

Tento článok bol pripravený v rámci podpory projektu APPV-22-0562 Posilnenie odolnosti kľúčových prvkov infraštruktúry využitím pokrokov v 3D modelovaní a IGP Hodnotenie odolnosti kľúčových prvkov kritickej infraštruktúry prostredníctvom pokroku v 3D modelovaní.

LITERATÚRA

[1] Zákon č. 135/1961 Z. z. o pozemných komunikáciách.

[2] BUJŇÁKOVÁ, P. 2020. Anchorage system in old post-tensioned precast bridges. In: Civil and Enviromental Engineering. Roč. 16, č. 2, s. 379-387. ISSN 13365835

[3] BUJŇÁKOVÁ, P., STRIEŠKA, M. 2017. Development of precast concrete bridges during the last 50 years in Slovakia. Procedia Engineering.

[4] Technické podmienky 059 Zadávanie a výkon diagnostiky mostov a lávok. 2024. Bratislava: MD SR. Dostupné na: https://www.ssc.sk/files/documents/technicke-predpisy/tp/tp_059_2023.pdf

[5] VIČAN, J., GOCÁL, J., ODROBIŇÁK, J., KOTEŠ, P. (2016). Analysis of Existing Steel Railway Bridges. Procedia Engineering, 156, pp. 507-514. doi: 10.1016/j.proeng.2016.08.328

[6] VIČAN, J., GOCÁL, J., ODROBIŇÁK, J., MORAVČÍK, M., KOTES, P. (2015). Determination of railway bridges loading capacity. Procedia Engineering 111, pp. 839-844.

[7] OTTAVIANO, E., REA, P. 2013. Design and operation of a 2-DOF leg-wheel hybrid robot. In: Robotica, Roč. 31, pp. 1319–1325.

[8] OTTAVIANO, E., REA, P., CASTELLI, G. 2014. THROO: a Tracked Hybrid Rover to Overpass Obstacles. In: *Advanced Robotics*, Roč.. 28, č. 10, Dostupné na: https://doi.org/10.1080/01691864.2014.891949

[9] REA, P., OTTAVIANO, E. 2023. Hybrid Inspection Robot for Indoor and Outdoor Surveys. In: *Actuators 2023*, Roč. 12, č. 108. Dostupné na: https://doi.org/10.3390/act12030108

[10] FIGULI, L. a kol. 2021. Recent developments on inspection procedures for infrastructure using UAVs. In: Modern Technologies Enabling Safe and Secure UAV Operation in Urban Airspace. ISBN 978-164368188-7

[11] Cestná databanka - *Dáta centrálnej technickej evidencie ciest so stavom dát k 1.1.2024*. [cit. 2024-12-20] [Online]. Bratislava: SSC. Available: https://www.cdb.sk/sk/statisticke-vystupy/2021.alej

[12] ŘEHÁK, D. a kol. 2018. Metodika hodnocení resilience prvků kritické infrastruktury. Ostrava: VŠB – Technická univerzita Ostrava, 2018. 90 s. ISBN 978-80-248-4164-9.

[13] HROMADA, M. 2010. Stanovení odolnosti kritickej infraštruktúry – teoretický rámec/Critical Infrastructure Resilience Determination – Theoretical Framework. In. Security Magazín. č. 93, str. 26-27. ISSN –1210-8723

[14] FIGULI, L. A DVOŘÁK, Z. 2023. Threats on the Critical Infrastructure Elements. In: Monitoring and protection of critical infrastructure by unmanned systems. ISBN 978-1-64368-377-5,2023. pp .238.

[15] ZLACKÁ, A. 2025. Korelačná závislosť. [cit. 02-04-2025] [Online]. Dostupné z: http://www.fhpv.unipo.sk/cvt/statistika/zlacka/geoinfo7.pdf

[16] TITKO, M., NOVÁK, L., JÁNOŠÍKOVÁ, M. 2021. Praktická štatistika. 1. edition. Žilina: EDIS – Publisher of UNIZA, 146 s. ISBN 978-80-554-1814-8.

[17] FIGULI, L. a kol. 2023. Posilnenie odolnosti kľúčových prvkov infraštruktúry využitím pokrokov v 3D modelovaní (REMAKE-3D). Dostupné na: https://www.remake3d.fri.uniza.sk

[18] DVOŘÁK, Z., CHOVANČÍKOVÁ, N., BRUK, J., M. HROMADA. 2021. Methodological Framework for Resilience Assessment of Electricity Infrastructure in Conditions of Slovak Republic [online]. In: *International Journal of Environmental Research and Public Health*. Available at: https://doi.org/10.3390/ijerph18168286

OCHRANA A TECHNICKÉ ZABEZPEČENÍ MALÝCH MODULÁRNÍCH JADERNÝCH ELEKTRÁREN V RÁMCI KRITICKÉ INFRASTRUKTURY ČR

Aleš Navrátil[1]

ABSTRAKT

V současnosti jsou jaderné elektrárny nedílnou součástí našeho každodenního života. S touto technologií přichází i velká zodpovědnost při jejich výstavbě a provozu. Výroba a distribuce elektrické energie je velmi důležitá pro růst ekonomiky a energetické soběstačnosti České republiky. Malé modulární reaktory jsou pro současnou bezpečnost a potřebu snížení počtu uhelných elektráren ideální volbou. Práce se snaží, popsat v základní míře úskalí ochrany a technické zabezpečení malých modulárních reaktorů v rámci kritické infrastruktury.

Kľúčové slová:
Jaderné elektrárny, modulární reaktory, kritická infrastruktura.

ABSTRACT

Today, nuclear power plants are an integral part of our daily lives. With this technology comes great responsibility in their construction and operation. The production and distribution of electricity is very important for the growth of the economy and energy self-sufficiency of the Czech Republic. Small modular reactors are the ideal choice for today's safety and the need to reduce the number of coal-fired power plants. This paper attempts to describe, at a basic level, the pitfalls of protection and technical security of small modular reactors within critical infrastructure.

Key words:
Nuclear power plants, modular reactors, critical infrastructure.

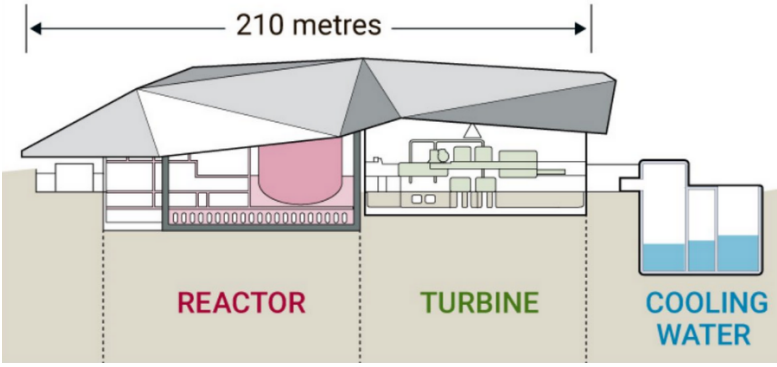
1 OCHRANA KRITICKÉ INFRASTRUKTURY

Česká republika prostřednictvím Skupinu ČEZ rozšiřuje zdrojovou základu nejen o novou výstavbu jaderných bloků, ale podporuje i technologii malých modulárních reaktorů (dále jen „SMR“). V současnosti se předpokládá vybudování první SMR v lokalitě jaderné elektrárny Temelín do konce 40. let [1].

1 Ing. Aleš Navrátil, Fakulta aplikované informatiky UTB, a1_navratil@utb.cz

1.1 TECHNOLOGIE MALÝCH MODULÁRNÍCH REAKTORŮ

Technické zabezpečení SMR bude srovnatelné s technickým zabezpečením velkých jaderných elektráren. Důležitým zákonem pro jadernou technologii a bezpečnost je zákon č. 263/2016 Sb. Zákon atomový zákon, který je doplněn vyhláškou 361/2016 Sb. Vyhláška o zabezpečení jaderného zařízení a jaderného materiálu [2].



Obrázek 12. Návrh jaderného reaktoru SMR společnosti Rolls-Royce [3].

1.2 DEFINOVÁNÍ A URČENÍ POJMU KRITICKÁ INFRASTRUKTURA

Pro podrobnější pochopení určování a ochranu kritické infrastruktury je důležité legislativní hledisko dané problematiky. V případě jaderných technologií se nejedná jen o národní, ale i o evropskou kritickou infrastrukturu.
Mezi důležité zákony a směrnice patří:

- Zákon č. 240/2000 Sb. Dle § 2 g) kritická infrastruktura [4],
- Nařízení vlády č. 432/2010 Sb. Dle § 1 [5],
- Zákon č. 181/2014 Sb. Dle § 2 b), Vymezení pojmů [6],
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury [7].

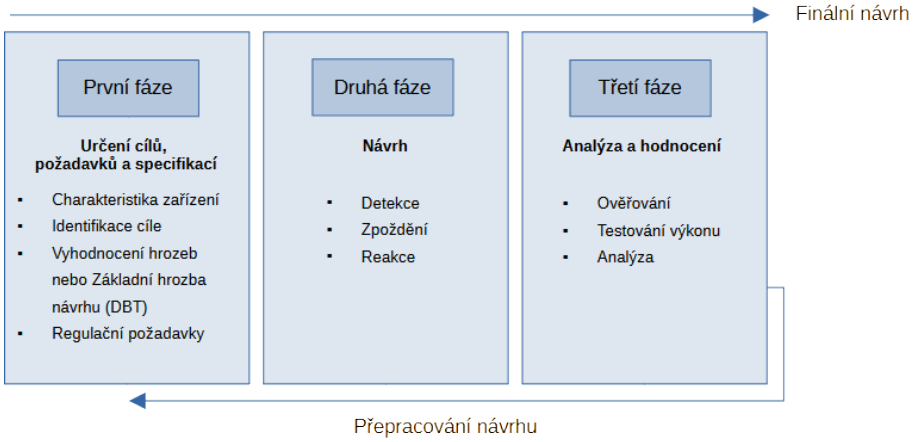
1.3 MALÉ MODULÁRNÍ REAKTORY A JEJICH BUDOUCÍ OCHRANA V RÁMCI KRITICKÉ INFRASTRUKTURY ČR

Obecně jsou jaderné elektrárny řazeny mezi nejstřeženějších objekty kritické infrastruktury České republiky [10].
Koncepce výstavby a zabezpečení SMR bude záležet na mnoha faktorech, které budou pro jednotlivé SMR rozdílné, například [11]:

- topografie,
- životní prostředí,
- hustota obyvatelstva v dané lokalitě,
- zdrojích elektromagnetického záření, které by mohlo rušit komunikační systémy (radiové nebo telefonní vysílače),
- přírodní seismické poruchy (podloží, geologické zlomy),
- povětrnostní podmínky pro danou lokalitu,
- určená jaderná uložiště,

- napojení na elektroenergetickou přenosovou soustavu.

Nejdůležitějším úkolem bude vytvoření bezpečnostních koncepcí, které budou garantovat technickou, kybernetickou a fyzickou bezpečnost v rámci kritické infrastruktury. V tomto případě se jedná o stanovení druhů potencionálních aktérů hrozeb s přihlédnutím pro danou lokalitu. Dále bude nutné definovat proces návrhu a hodnocení systému zabezpečení [11, 12].



Obrázek 13. Proces návrhu a hodnocení systému zabezpečení [11].

Systém řízení ochrany, který vychází z jednotlivých procesních kroků pro stanovení optimalizace bezpečnosti je rozdělen na [13]:

Analytická část
- klasifikace a ohodnocení aktiv,
- definice katalogu hrozeb a rizik kritické infrastruktury,
- analýza a hodnocení rizik.

Návrhová část
- stanovení katalogu bezpečnostních opatření (kategorizace a parametry),
- stanovení požadavků a návrh systému řízení ochrany.

1.3.1 ANALYTICKÁ ČÁST

Klasifikace a řízení životního cyklu aktiv jsou důležitým vektorem k zajištění bezpečnosti SMR. Jedná se o soubor technicko- ekonomických studií, analýzy rizik, údržby majetku, optimalizaci nákladů a dodavatelské řetězce. Všechny tyto aktiva musí mít shodu s nastavenou interní bezpečnostní politikou [14]. V oblasti externích aktiv se může jednat například o distribuční soustavu elektrické energie [15].

Pro provoz SMR bude dostupná, stabilní a zabezpečená distribuční síť velice důležitá. Distribuční síť bude zajišťovat nejen přenos elektrické energie z jaderné elektrárny ke spotřebiteli, ale bude sloužt také k procesům v samotné SMR, například k chlazení jaderného reaktoru [15].

Základní doporučení pro externí a interní distribuční síť s ohledem na bezpečný provoz SMR [15; 16]:

- stabilita frekvence a výkonu distribuční sítě – nestabilita může například vést k přehřátí a vypnutí ochranných systémů (malé výkonnostní pásmo). Jedná se například o záměrné poškozování distribuční sítě (sabotáž, teroristický útok),
- zabezpečení záložních energetických zdrojů při výpadku distribuční sítě (chlazení SMR, záložní zabezpečovací systémy),
- dostatečné energetická rezerva v případě odstávky SMR.

Životní cyklus aktiv SMR [15]:

- nastavení pravidel směřující k zajištění vysoké úrovně spolehlivosti,
- nastavení procesů k dlouhodobému ekonomického využití,
- zajištění dostatečného kapitálu pro bezpečný a stabilní provoz,
- nastavení monitorovacích a bezpečnostních procesů.

1.3.2 NÁVRHOVÁ ČÁST

Jedná se o oblast návrhu bezpečnostních opatření kritické infrastruktury, které budou zajišťovat ochranu SMR v rámci kritické infrastruktury.

Mezi oblasti bezpečnostních opatření kritické infrastruktury můžeme zahrnout [11; 14]:

- Administrativní bezpečnost – pravidla administrativní bezpečnosti jsou stanovena zákonem č. 412/2005 § 21 - § 23, Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Dále se jedná o vyhlášku č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informacích [17].
- Fyzická bezpečnost – jedná se o návrh zabezpečovacích systémů stanovených dle procesů a metodik, které jsou v souladu s normativními požadavky. Při tvorbě koncepce fyzické bezpečnosti je důležité, jak nejlépe zkombinovat opatření týkající se typů a umístění technických zabezpečovacích systémů, například bariér, senzorů, kamerových systémů, komunikačních zařízení a záložních systémů. Komplexním cílem je vyváženost mezi funkcemi detekce, zpožděním a reakcí umožňující efektivní funkčnost celého bezpečnostního systému [11]. Pravidla jsou také obsažena v zákoně č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů [18].
- Kybernetická bezpečnost – bezpečnost informačních systémů SMR hrají významnou roli při zabezpečení provozu a činností využívajících, skladujících a přepravujících jaderný a jiný radioaktivní materiál [19].

Mezi důležité zákony, směrnice a vyhlášky v rámci kybernetické bezpečnosti SMR můžeme zařadit [19]:

- **zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti),**

- **směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Směrnice NIS),**
- vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti,
- nová vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti,
- **vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích,**
- **vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby,**
- **vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu,**
- **vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci,**
- **vyhláška č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu,**
- **prováděcí nařízení EK ke Směrnici NIS, které stanoví bezpečnostní opatření a parametry významnosti dopadu incidentu pro poskytovatele digitálních služeb.**

Klíčové zranitelnosti budoucí SMR s pohledu kybernetické bezpečnosti [20]:

- personální a fyzická zranitelnost,
- celoodvětvová a kulturní zranitelnost,
- technická zranitelnost – technologie umělé inteligence, kvantově prolomitelné šifry nebo nové typy hrozeb [21, 22].

Atributy a charakteristiky kybernetické hrozby pro budoucí SMR [19, 20]:

- motivace: politická, finanční, ideologické nebo osobní,
- záměr:
    - sabotáž radioaktivního materiálu,
    - sabotáž radioaktivního zařízení,
    - krádež radioaktivního nebo jaderného materiálu,
    - vyvolání paniky (sociální rozvrat),
    - vyvolání politické nestability.
- znalosti: znalost architektury informačních komunikačních technologií, znalost bezpečnostních opatření a postupů radiační ochrany SMR.
  Kybernetická hrozba je jedinečná v tom, že nebude vznikat v bezprostřední blízkosti SMR. Tato hrozba není také závislá na počtu útočníků a umístění samotné SMR [19, 20].

Trendy potencionálních hrozeb [19, 20]:

- rostoucí počet útočníků provádějících sofistikované útoky s minimálními náklady (anonymní pronájem virtuálních výpočetních služeb),
- rostoucí počet nabízených nelegálních služeb (Dark Web),
- pokračující využívání sociálního inženýrství.

Hlavní kybernetické hrozby pro budoucí SMR [19, 20]:

- vnitřní hrozba (zasvěcená osoba): zaměstnanec s určitým přístupovým oprávněním,
    - přístup k aktivům,
    - přístup k technickým a bezpečnostním dokumentacím,
    - znalost vnitřních procesů.
- extrémista: osamocený nebo volně koordinovaný útok,
- reakční hacker: jednotlivec nebo skupina s motivací zviditelnění vlastních schopností (kompromitace systému nemusí být cílená),
- organizovaný zločin: cílem je peněžní zisk (prodej informací),
- nepřátelská státní moc: trvalá hrozba,
- terorismus: zaměření na narušení zabezpečení (sabotáž).

Personální bezpečnost – personální bezpečnost upravuje Vyhláška č. 363/2011 Sb. Vyhláška o personální bezpečnosti a o bezpečnostní způsobilosti [23]. Jedná se o koncepci minimalizovat dopad lidských chyb, krádeží, podvodů, teroristických útoků nebo zneužití informačních prostředků. Personální bezpečnost stanovuje tyto oblasti [11, 13]:

- odpovědnosti, povinnosti a pravomoci,
- prověřování zaměstnanců,
- dohoda o ochraně informací,
- školení zaměstnanců,
- disciplinární proces.

ZÁVĚREM

Práce popisuje základní principy ochrany a bezpečnosti malých modulárních jaderných elektráren. Je důležité zohlednit změny, které budou předcházet výstavbě těchto zařízení. Bude se jednat o změny v legislativě, v konceptu bezpečnostních technologiích a v nárocích na výběr požadovaného personálu. Samotná technologie a zabezpečení modulárních reaktorů je již známá a v dostatečné míře zvládnutá. Příkladem mohou být například jaderné ponorky. V případě malých modulárních reaktorů se bude jednat o ostrovní systémy, které budou vyžadovat technické zabezpečení v oblastech s větší hustotou osídlení. Důležitým úkolem bude také stanovení bezpečnostních procesů a principů, které budou minimalizovat technické nebo personální selhání. Závěrem lze konstatovat, že technologie malých modulárních jaderných elektráren je důležitým energetickým směrem v rámci budoucnosti České republiky.

LITERATÚRA

[1] Malé modulární reaktory. Online. ČEZ. 2025. Dostupné z: https://www.cez.cz/cs/nove-jaderne-zdroje/male-modularni-reaktory/co-jsou-male-modularni-reaktory. [cit. 2025-01-26].

[2] Často kladené otázky. Online. SKUPINA ČEZ. 2025. Dostupné z: https://www.cez.cz/cs/nove-jaderne-zdroje/male-modularni-reaktory/casto-kladene-otazky. [cit. 2025-01-22].

[3] SMALL MODULAR REACTORS (SMR). Online. Foreningen Atom-kraft Ja Tak. 2025. Dostupné z: https://rpmanetworks.com/atomkraftclonesite-english/docs/small-modular-reactors-smr/. [cit. 2025-01-26].

[4] Zákon č. 240/2000 Sb. Zákon o krizovém řízení a o změně některých zákonů (krizový zákon). Online. Zákony pro lidi. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-240. [cit. 2025-04-02].

[5] Nařízení vlády č. 432/2010 Sb. Nařízení vlády o kritériích pro určení prvku kritické infrastruktury. Online. Zákony pro lidi. Dostupné z: https://www.zakonyprolidi.cz/cs/2010-432. [cit. 2025-04-02].

[6] Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Online. Zákony pro lidi. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181. [cit. 2025-04-02].

[7] Návrh zákona o odolnosti subjektů kritické infrastruktury a o změně dalších zákonů (zákon o kritické infrastruktuře). Online. Technicka-zarizeni. 2024. Dostupné z: https://www.technicka-zarizeni.cz/navrh-zakona-o-odolnosti-subjektu-kriticke-infrastruktury-a-o-zmene-dalsich-zakonu-zakon-o-kriticke-infrastrukture/. [cit. 2025-03-05].

[8] Vyhláška č. 317/2014 Sb. Vyhláška o významných informačních systémech a jejich určujících kritériích. Online. Zákony pro lidi. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-317. [cit. 2025-04-02].

[9] 32024R1689. Online. Zákony pro lidi. Dostupné z: https://www.zakonyprolidi.cz/pravoeu/dokument/souvislosti?celex=32024R1689&date=0. [cit. 2025-04-02].

[10] Často kladené otázky. Online. SKUPINA ČEZ. 2025. Dostupné z: https://www.cez.cz/cs/nove-jaderne-zdroje/male-modularni-reaktory/casto-kladene-otazky. [cit. 2025-01-22].

[11] Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities. Online. IAEA - International Atomic Energy Agency. 2021. Dostupné z: https://www.iaea.org/publications/13459/handbook-on-the-design-of-physical-protection-systems-for-nuclear-material-and-nuclear-facilities. [cit. 2025-01-22].

[12] Design Basis Threat (DBT). Online. IAEA - International Atomic Energy Agency. 2024. Dostupné z: https://www.iaea.org/topics/security-of-nuclear-and-other-radioactive-material/design-basis-threat. [cit. 2025-01-22].

[13] Metodika zajištění ochrany kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie. Online. Ministerstvo vnitra České republiky. 2012. Dostupné z: https://mv.gov.cz/chh/clanek/ochrana-kriticke-infrastruktury-ochrana-kriticke-infrastruktury.aspx. [cit. 2025-03-12].

[14] Řízení aktiv. Online. Skupina ČEZ. 2025. Dostupné z: https://www.cez.cz/udrzitelnost-a-etika/cs/governance/rizeni-aktiv. [cit. 2025-03-12].

[15] ELECTRIC GRID RELIABILITY AND INTERFACE WITH NUCLEAR POWER PLANTS. Online. IAEA - International Atomic Energy Agency. 2012. Dostupné z: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1542_web.pdf. [cit. 2025-03-17].

[16] Grid Stability and Safety Issues Associated with Nuclear Power Plants. Online. Nautilus. 2011. Dostupné z: https://www.nautilus.org/wp-content/uploads/2011/12/Bickel.pdf. [cit. 2025-03-17].

[17] Informace. Online. NBÚ. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/223-administrativni-bezpecnost-tvorba-prijem-evidence-2/1277-informace-2/. [cit. 2025-03-13].

[18] Informace k fyzické bezpečnosti. Online. NBÚ. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost-technicke-prostredky-a-dalsi-prvky-fyzicke-bezpecnosti-a-jejich-certifikace/1014-informace/. [cit. 2025-03-13].

[19] Legislativa KB. Online. NÚKIB - Národní úřad pro kybernetickou bezpečnost. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/. [cit. 2025-03-14].

[20] Cybersecurity of the civil nuclear sector. Online. Chatham House. 2025. Dostupné z: https://www.chathamhouse.org/2024/07/cybersecurity-civil-nuclear-sector/2-threats-and-risks-civil-nuclear-infrastructure. [cit. 2025-03-14].

[21] Portál NÚKIB nově podporuje kvantově odolnou kryptografii. Online. NÚKIB - Národní úřad pro kybernetickou bezpečnost. 2024. Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/2156-portal-nukib-nove-podporuje-kvantove-odolnou-kryptografii/. [cit. 2025-03-15].

[22] MINIMÁLNÍ POŽADAVKY NA KRYPTOGRAFICKÉ ALGORITMY. Online. NÚKIB. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Minimalni_pozadavky_v4_FINAL.pdf. [cit. 2025-04-02].

[23] Vyhláška č. 363/2011 Sb. Vyhláška o personální bezpečnosti a o bezpečnostní způsobilosti. Online. Zákony pro lidi. Dostupné z: https://www.zakonyprolidi.cz/cs/2011-363. [cit. 2025-04-03].

THE IMPACT OF NIS2 DIRECTIVE ON THE RESILIENCE OF CRITICAL INFRASTRUCTURE ENTITIES

Mimi Enakome Oka[1], Martin Hromada[2], Roman Jasek[3]

ABSTRACT

The Network and Information Security Directive 2 (NIS 2), adopted by the European Parliament in November 2022 and implemented in 2024, strengthens cybersecurity regulations across the European Union by addressing the limitations of its predecessor, NIS 1. The previous directive left some sectors unregulated, leading to inconsistent cybersecurity investments and fragmented implementation across member states. NIS 2 expands the scope of covered entities, introduces clearer cybersecurity requirements, and mandates stricter enforcement to enhance the resilience of essential services. While the directive aims to improve risk management, incident reporting, and supply chain security, its transposition into national law allows for variations in implementation. This paper assesses the impact of NIS 2 on the resilience of critical infrastructures, highlighting its effectiveness in mitigating cyber risks and examining key challenges such as compliance costs, the burden on essential service providers to audit suppliers, technical expertise gaps, and policy alignment among member states. The findings underscore NIS 2's role in fostering a proactive cybersecurity culture while identifying areas for improvement to ensure long-term protection against evolving cyber threats.

Key words
Network and Information Security Directive (NIS) 1 and 2, European Union Agency for Cybersecurity (ENISA), Cybersecurity Framework, Critical Infrastructures, Cyber Resilience.

1 INTRODUCTION

The growing digital dependencies of modern society have significantly expanded the cyber threat landscape, making cybersecurity management increasingly complex. The steady rise in users, interconnected systems, and digital services has introduced new vulnerabilities, providing greater opportunities for

1 Mimi Enakome Oka, Tomas Bata University Zlin, Faculty of informatics, Tel: +420739976369, oka@utb.cz
2 Prof. Martin Hromada, Tomas Bata University Zlin, Faculty of informatics, Tel: +420608454732, hromada@utb.cz
3 Prof. Roman Jasek, Tomas Bata University Zlin, Faculty of informatics, Tel: +420576035376, jasek@utb.cz

cyber-dependent crime. Recognizing these challenges, the NIS 1 Directive was adopted in 2016 to strengthen cybersecurity across the European Union. However, it faced several limitations, prompting the adoption of NIS 2, which aims to establish a higher common level of cybersecurity by addressing regulatory gaps, expanding sectoral coverage, and enhancing enforcement mechanism [1].

One of the primary weaknesses of NIS 1 was its limited scope, as it applied only to certain digital service providers (DSPs) and operators of essential services (OESs). The narrow applicability overlooked the increasing dependencies between sectors, leaving many critical industries outside their regulatory framework. As a result, companies not covered by the directive had no legal obligation to meet cybersecurity standards despite their significance in ensuring overall security [2]. NIS 2 addresses this gap by expanding its scope, introducing Essential Entities (EE) and Important Entities (IE), and establishing a more structured governance framework at the national level [1].

The directive now includes additional sectors such as wastewater management, public administration, space, and chemical manufacturing, while also incorporating a size threshold to determine applicability [2].

NIS 1 introduced a risk-based approach for cybersecurity measures and incident reporting, its implementation varied significantly among Member States. Some nations introduced detailed security requirements, while others provided minimal guidance, leading to inconsistent standards [2]. Additionally, the absence of common criteria for evaluating security measures and incidents contributed to uncertainties. Under NIS 2, reporting obligations are expanded to include incidents capable of causing severe operational disruption or financial losses [2]. Organizations must now report incidents within 24hrs for early warnings, within 72 hours for official notification, and submit a final report within one month. This shift ensures that cybersecurity incidents are promptly identified, shared, and mitigated to enhance future resilience [1].

Another major improvement in NIS 2 is the emphasis on national-level cooperation. While NIS 1 primarily facilitated collaboration among competent cybersecurity authorities, Single Points of Contact (SPOCs), and Computer Security Incident Response Teams (CSIRTs), NIS 2 strengthens coordination with law enforcement, data protection authorities, and other relevant bodies, recognizing the previous reluctance to share cybersecurity threat information, the new directive introduces a dedicated chapter on information sharing, encouraging greater transparency and collaboration among stakeholders [2].

To ensure a uniform standard of cybersecurity enforcement, NIS 2 expands the powers of national cybersecurity authorities [1]. Member States must ensure that competent authorities have the power to issue warnings, enforce binding instructions, and impose administrative fines. Penalties can reach EUR 10 million or 2% of the total worldwide annual turnover, strengthening regulatory oversight [2].

Despite its advancements, the NIS 2 Directive presents several challenges in its implementation. One key concern is the requirement for management-level cybersecurity training. While awareness is crucial, many covered entities already have dedicated IT and security teams. The directive mandates training in cybersecurity risk assessment and management, which are highly technical topics that may not be directly relevant to all management personnel. Implementing such training could prove resource-intensive, particularly for organizations without prior cybersecurity expertise [1].

Additionally, the expanded scope and stricter requirements under NIS 2 will increase regulatory burdens, leading to higher costs even for entities that previously invested in cybersecurity under NIS 1. Organizations in newly covered sectors will face significant financial and operational adjustments to meet compliance standards [1].

This research paper seeks to examine the impact of NIS 2 on cybersecurity resilience by addressing the following key questions:

- RQ1: What are the challenges associated with the implementation of NIS 2, particularly regarding compliance costs, supply chain security, and technical expertise?
- RQ2:To what extent does NIS 2 improve incident reporting for critical infrastructure organizations?
- RQ3: What are the potential gaps in NIS 2 that may limit its effectiveness in mitigating evolving cyber threats?

2 LITERATURE REVIEW

The NIS 2 Directive introduces a broad set of cybersecurity regulations, and several scholars have examined its scope, enforcement mechanisms, and implications.

2.1 SCOPE, ENFORCEMENT, AND FINANCIAL IMPACT OF NIS 2

Key aspects of the NIS 2 Directive, particularly its scope, enforcement mechanisms, and cost implications have been analyzed by some researchers. The directive generally excludes entities with fewer than 50 employees and an annual turnover below EUR 10 million. While acknowledging that size is not a perfect measure of an entity's criticality, the Commission considers it a meaningful proxy for determining an entity's importance to society and the economy. However, exceptions exist—certain entities remain within the directive's scope regardless of size, such as small companies that are the sole producers of critical goods within an EU Member State [3].

Also, the legal and professional accountability of management personnel under NIS 2 was examined. National Competent Authorities (NCAs) have the power to impose professional bans on executives of essential entities and hold them personally liable for failing to ensure compliance. However, the scope of this

liability remains legally ambiguous, particularly concerning whether it extends to third-party civil liability or remains limited to employer-employee obligations [3].

Regarding the financial impact of NIS 2, the European Commission estimates that newly included entities will face a cost increase of approximately 0.63% of their total turnover, while those already covered under NIS 1 will see an increase of 0.58%. The primary cost driver is compliance with cybersecurity requirements, which do not differentiate between essential and important entities. Differentiating these requirements could improve cost efficiency by aligning obligations with the varying risk levels and resource capacities of different entities [3].

Finally, the expanded scope of NIS 2 will place greater demands on NCAs, requiring additional financial and human resources to maintain effective supervision. Even though the directive removes the identification process for regulated entities, NCAs still need sufficient resources to oversee compliance and enforcement [3].

2.2 SUPPLY CHAIN CYBERSECURITY UNDER NIS 2

The NIS 2 Directive lacks clarity in defining supply chain cybersecurity measures. The directive does not explicitly outline the roles of focal companies or governing entities within a supply chain, raises concerns about its ability to effectively mitigate cybersecurity risks [4].

Under Article 21, IoT-using entities must assess the cybersecurity vulnerabilities of their direct suppliers and service providers. However, the directive does not specify which suppliers qualify as direct suppliers, leading to ambiguity in its application [4].

Furthermore, while the directive mandates an "all-hazard risk management approach" that includes supply chain security and supplier relationships, the broad wording leaves room for interpretation. This ambiguity means that supply chain cybersecurity measures could range from preventing hardware tampering to addressing software vulnerabilities [4].

Moreover, NIS 2 lacks a precise definition of the scope and extent of supply chain cybersecurity. Various interpretations exist regarding when the cybersecurity process begins and ends. The Council of the EU defines it as beginning with raw material sourcing and extending through manufacturing, processing, delivery, and ongoing support throughout a product’s lifecycle. This interpretation suggests that continuous security updates for IoT devices should be required to quickly patch vulnerabilities and reduce cyber threats. However, NIS 2 does not explicitly confirm whether such ongoing support falls under its supply chain cybersecurity obligations [4].

2.3 REGULATORY ALIGNMENT: THE CYBER RESILIENCE ACT AND NIS 2

The Cyber Resilience Act (CRA) complements the NIS 2 Directive by strengthening cybersecurity standards for products with digital elements. The CRA applies to all such products and aims to assist essential and important entities in meeting strict due diligence requirements. By placing greater responsibility on manufacturers, the CRA ensures that hardware and software products meet high cybersecurity standards before reaching the market [5].

Although NIS 2 entities remain responsible for assessing their suppliers, the CRA helps establish a baseline level of security in the products they use [5]. Another significant issue addressed by the CRA is the lack of transparency regarding the security properties of digital products. Essential and important entities often struggle to obtain sufficient information about cybersecurity features, which hinders their ability to make informed purchasing decisions and fulfill due diligence obligations. To address this, the CRA introduces new transparency requirements, obliging manufacturers to prepare technical documentation before placing their products on the market. This increased transparency is expected to help NIS 2 entities identify reliable products more easily [5].

Finally, the European Commission anticipates that the CRA will result in significant cost savings for NIS 2 entities by improving cybersecurity across supply chains. By ensuring that products with digital elements meet higher security standards, the CRA reduces the burden on essential and important entities to implement additional security measures [5].

3 METHODOLOGY

This study conducted a qualitative analysis of three white papers examining the implementation and impact of the NIS 2 Directive: (1) Report on the State of Cybersecurity in the European Union, (2) the ECSO NIS 2 White Paper, and (3) the KPMG NIS 2 White Paper. These documents were selected based on their relevance to key aspects of NIS 2, including risk management, compliance costs, and incident reporting.

Using thematic analysis, excerpts related to these three categories were identified and systematically coded to extract recurring themes. Under risk management, the analysis revealed themes such as the need for unified implementation and stakeholder engagement, cyber-security maturity and compliance challenges, a risk-based and proportional approach to security, and governance and supervision. In the category of compliance costs, key themes included fragmented implementation across the EU, lack of organizational readiness and budgetary constraints, strict enforcement and executive accountability, the need for training and awareness programs, and the role of information sharing and external support. Regarding incident reporting, the analysis identified underreporting of incidents and reluctance among SMEs to

disclose cyberattacks, as well as gaps in cooperation between NIS2 and other regulatory authorities.
A secondary level of thematic analysis was conducted to identify overarching patterns across the three areas, resulting in four central findings:

1. Fragmented implementation across the EU has led to uncertainty and compliance difficulties.
2. Budgetary constraints and lack of resources hinder both organizations and regulators from achieving full compliance with NIS 2.
3. A unified approach to cybersecurity frameworks is necessary to streamline compliance and enhance security resilience.
4. Organizations may struggle to meet NIS 2's strict incident reporting deadlines due to insufficient infrastructure and unclear guidelines.

This approach ensured a structured and systematic exploration of the white papers, allowing for the identification of common challenges and trends in NIS 2 implementation.

4 ANALYSIS AND DISCUSSION

4.1 CHALLENGES ASSOCIATED WITH NIS 2 IMPLEMENTATION (RQ1)

The implementation of the NIS 2 Directive presents several challenges, particularly concerning compliance costs, supply chain security, and technical expertise. Nearly three – quarters of organizations lack dedicated implementation budgets, while one-third report report no direct involvement from management despite legal obligations [6]. Without sufficient financial and human resources, organizations struggle to adopt the necessary cybersecurity measures, weakening overall resilience.

Supply chain security also poses a major challenge. Organizations often struggle to identify and categorize significant incidents originating from third-party vendors, delaying incident reporting and increasing regulatory risks [6]. Given that supply chains are highly interconnected, a lack of uniform cybersecurity standards among vendors further complicates compliance efforts. Additionally, technical expertise remains a concern, as many newly regulated sectors face a steep learning curve in understanding and implementing NIS 2 requirements.

4.2 IMPROVEMENTS IN INCIDENT REPORTING (RQ2)

One of the primary objectives of NIS 2 is to strengthen incident reporting for critical infrastructure organizations. The structured reporting framework aims to enhance cybersecurity response coordination across Member States.

However, challenges remain, some Memeber States still lack dedicated reporting tools, which hinder organizations' ability to comply with reporting timelines [7]. Moreover, the requirement to assess the severity and impact of an incident within a short time frame can be difficult for organizations with limited

technical expertise. Also, SMEs in particular, are reluctant to disclose cyberattacks, fearing reputational damage or financial repercussions, which may undermine the effectiveness of NIS 2's incident reporting measures [6].

4.3 Potential Gaps in NIS 2's Effectiveness Against Evolving Cyber Threats (RQ3)

Despite its strengthened regulatory framework, NIS 2 has several gaps that may limit its long-term effectiveness in mitigating cyber threats. One key issue is the fragmented implementation across EU Member States. As of December 2024, only four countries—Croatia, Italy, Belgium, and Lithuania—had fully transposed the directive, while most others targeted Q1 2025 for adoption [6]. This staggered approach creates inconsistencies in enforcement, making it difficult for multinational organizations to maintain compliance across different jurisdictions.

Notably there are gaps in cooperation between NIS 2 authotities and other regulatory bodies, limiting the directive's ability to align with broader cybersecurity and data protection frameworks [7]. This lack of integration could result in regulatory overlaps or conflicting requirements, increasing compliance burdens on organizations.

5 CONCLUSION AND FURTHER RESEARCH

The findings of this study indicates that while the NIS 2 Directive strengthens cybersecurity regulations and promotes a unified approach to compliance, several challenges hinders its full effectiveness. Financial and resource contraints, fragmented implementation across Members States, and compliance burdens create significant barriers to seamless adoption. Additionally, while the directive enhances risk management and incidence response, its rigid compliance structure and reliance on existing cyberseurity frameworks may limit its adaptability to rapidly evolving cyber threats, such as AI–driven attacks and sophisticated supply chain compromises.

A critical challenges remains in supply chain security, where critical infrastructures bear the burden of ensuring third- party compliance, despite limited guidance and enforcement mechanisms. Moreover, cross – border regulatory inconsistencies create uncertainty for multinational organizations, making compliance more complex.

Continuous regulatory updates, enhanced co-ordination across Member States, and increased investments in cybersecurity infrastructure are essential to ensuring the effectiveness of NIS 2. Future research should focus on empirical studies examining sector- specific adoption, cross border regulatory comparisons, the effectiveness of incident reporting mechanisms, and practical solutions for overcoming compliance barriers.

REFERENCES

[1] Vandezande N, 2024. “Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor,” *Comput. Law Secur. Rev.*, vol. 52, p. 105890, Apr. 2024, doi: 10.1016/j.clsr.2023.105890.

[2] Schmitz-Berndt S and Cole M, 2022. “Towards an Efficient and Coherent Regulatory Framework on Cybersecurity in the EU: The Proposals for a NIS 2.0 Directive and a Cyber Resilience Act,” *Appl. Cybersecurity Internet Gov.*, vol. 1, no. 1, pp. 1–17, Dec. 2022, doi: 10.5604/01.3001.0016.1323.

[3] Sievers T, 2021. “Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations,” *Int. Cybersecurity Law Rev.*, vol. 2, no. 2, pp. 223–231, Dec. 2021, doi: 10.1365/s43439-021-00033-8.

[4] Anon M, 2024. “The Regulation of Supply Chain Cybersecurity in the NIS2 Directive in the Context of the Internet of Things,” *SSRN Electron. J.*, 2024, doi: 10.2139/ssrn.4848048.

[5] Eckhardt P and Kotovskaia A, 2023. “The EU’s cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive,” *Int. Cybersecurity Law Rev.*, vol. 4, no. 2, pp. 147–164, Jun. 2023, doi: 10.1365/s43439-023-00084-z.

[6] ECSO, NIS2-White Paper European Cybersecurity Organisation 2024 .

[7] European Union Agency for Cybersecurity 2024*. report on the state of cybersecurity in the Union.* LU: Publications Office, 2024. Accessed: Mar. 23, 2025. [Online]. Available: https://data.europa.eu/doi/10.2824/0401593

[8] Bella G, Castiglione G, and Santamaria D. F,2023. “An Ontological Approach to Compliance Verification of the NIS 2 Directive”, doi: 10.48550/aXiv.2307.01211.

[9] Biasin E and Kamenjaševic E, 2022 “Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals,”.

[10] Schmitz-Berndt S, 2023. “Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive,” *J. Cybersecurity*, vol. 9, no. 1, p. tyad009, Jan. 2023, doi: 10.1093/cybsec/tyad009.

[11] European Union Directive (EU) 2022/2555 on Measure for a high common level of cybersecurity across the union, Official Journal of European Union L333/80. Dec 2022.”

[12] Malatras A, “EU cybersecurity index,” 2024 European Union Agency for Cybersecurity (ENISA).

[13] Purser S, 2016.“Implementing the NIS Directive driving cybersecurity improvements for Essential Services” (ENISA).

[14] European Union Aency for Cybersecurity (ENISA), 2024. “NIS Directive Cyber Assessment Framework.”

[15] Maglaras L, Drivas G, Noou K, and Rallis S,2018. “NIS directive: The case of Greece,” vol. 4, no. 14, 2018.

[16] Schmitz-Berndt S and Chiara P.G., 2022. “One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive,” *Int. Cybersecurity Law Rev.*, vol. 3, no. 2, pp. 289–311, Dec. 2022, doi: 10.1365/s43439-022-00058-7.

[17] Wanecki P, Jašek R, and Drofova I, 2023. “The Contribution of the European NIS2 Directive to the Design of the Cyber Security Model,” in *2023 International Conference on Information and Digital Technologies (IDT)*, Zilina, Slovakia: IEEE, Jun. 2023, pp. 149–154. doi: 10.1109/IDT59031.2023.10194454.
[18] Cole M D and Schmitz S, 2019. “The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape,” *SSRN Electron. J.*, 2019, doi: 10.2139/ssrn.3512093.
[19] Ferguson D. D. S, 2023. “The outcome efficacy of the entity risk management requirements of the NIS 2 Directive,” *Int. Cybersecurity Law Rev.*, vol. 4, no. 4, pp. 371–386, Dec. 2023, doi: 10.1365/s43439-023-00097-8.
[20] KPMG, EU NIS 2 Report, 2024.

MOŽNOSTI ZVYŠOVANIA BEZPEČNOSTI NA ELEKTRIČKOVÝCH TRATIACH

Peter Onderčo[1], Jan Rybář[2], Jozef Leja[3]

ABSTRAKT

Príspevok sa zaoberá bezpečnosťou v mestách, ktoré prevádzkujú električkovú dopravu. Bezpečnosť na električkových tratiach sa týka nielen električiek, ktoré na tratiach premávajú, ale aj cestujúcich, ktorý sa v električkách presúvajú z bodu „A“ do bodu „B“, ďalej účastníkov cestnej premávky, cyklistov a tých najzraniteľnejších, chodcov. Z každej mimoriadnej udalosti, ktorá sa na trati stane, sa vyvodzujú dôsledky v podobe nových bezpečnostných opatrení, či už do samotných vozidiel, alebo do okolia trate, aby sa do budúcna predchádzalo práve mimoriadnym udalostiam, ktoré môžu ohroziť život cestujúcich v električke, vodiča a ostatných účastníkov cestnej premávky. Cieľom príspevku je analyzovať bezpečnostné prvky na električkových tratiach, ďalej poukázať na vybrané nedostatky týkajúce sa bezpečnosti a navrhnúť možnosti pre zvýšenie bezpečnosti.

Kľúčové slová:
bezpečnosť, električka, manažment rizík, mimoriadna udalosť

ABSTRACT

The paper deals with safety in cities that operate tram transport. Safety on tram lines concerns not only the trams that run on the tracks, but also the passengers who move from point “A“ to point “B“ in the trams, as well as road users, cyclists and the most vulnerable, pedestrians. From every extraordinary event that happens on the track, consequences are drawn in the form of new safety features, either to the vehicles themselves or to the surroundings of the track, in order to prevent extraordinary events in the future that can endanger the lives of tram passengers, the driver and other road users. The aim of the contribution is to analyze the safety features on tram lines, to further point out selected deficiencies related to safety and to suggest options for increasing safety.

Key words:
safety, tram, risk management, extraordinary event

1 Ing. Peter Onderčo, Strojnícka fakulta, Slovenská technická univerzita v Bratislave, Nám. slobody 17, 812 31, Bratislava, +421 911 291 630, peter.onderco@stuba.sk
2 doc. Mgr. Ing. Jan Rybář, PhD., Strojnícka fakulta, Slovenská technická univerzita v Bratislave, Nám. slobody 17, 812 31, Bratislava, +421 949 611 537, jan.rybar@stuba.sk
3 RNDr. Jozef Leja, PhD., Strojnícka fakulta, Slovenská technická univerzita v Bratislave, Nám. slobody 17, 812 31, Bratislava, +421 948 210 850, jozef.leja@stuba.sk

1 ÚVOD DO RIEŠENEJ PROBLEMATIKY

Električková doprava v porovnaní s vlakovou dopravou jazdí v mestách, ktoré majú pre daný typ dopravy vybudovanú infraštruktúru. Priemerná rýchlosť dopravy v meste závisí od aktuálnej situácie, ale vieme povedať, že je rádovo nižšia ako doprava na železnici. Priemernú rýchlosť električiek sa snažia mestá zvyšovať, s čím ale priamo súvisí aj bezpečnosť na tratiach a kvalita poskytovaných služieb. Čím je vyššia rýchlosť električkovej dopravy, tým sa priamo zvyšuje aj kvalita poskytovaných služieb v závislosti s časom prepravy, ale tým sa priamo znižuje aj bezpečnosť na trati, na ktorú je potrebné klásť väčší dôraz. Keďže je ale električková doprava pomalšia než železničná nevyžaduje si toľko zabezpečovacích prvkov ako železnica.

2 BEZPEČNOSTNÉ PRVKY NA TRATI

Momentálny stav vztiahnutý na električkovú dopravu nie je nastavený správne, nebezpečné situácie vznikajú na dennej báze. Pre správne nastavenie zvyšovania bezpečnosti, je potrebné určiť komu chceme tú bezpečnosť zabezpečiť. Rozdelili sme si účastníkov na električkovej trati do 4 hlavných kategórií. Tieto kategórie postupne analyzujeme, ako sú chránení teraz a ako by mohli byť ochránení viac. Chodci a cyklisti sú prvá kategória, ďalej máme kategóriu individuálnej automobilovej dopravy (IAD), do ktorej spadá celá cestná doprava, ďalej samotní cestujúci, ktorí sa vezú v električke a v neposlednom rade vodič spoza panela električky [1].

2.1 CHODCI A CYKLISTI

Chodci a cyklisti tvoria najzraniteľnejšiu skupinu účastníkov cestnej dopravy a preto kladieme na ich bezpečnosť najväčší dôraz. Takisto ako pri klasických prechodoch pre chodcov je potrebné sa presvedčiť či môžu vstúpiť na vozovku. Toto pravidlo platí dvojnásobne pri prechode cez električkovú trať. Potrebné je takisto podotknúť, že električková trať sa smie prechádzať len na určených miestach. Či už sú to organizované prechody so semaformi, mimoúrovňové prechody alebo v okolí zastávok vyasfaltované prechody pre chodcov. Na väčšine neriadených prechodov sa nachádzajú aj bezpečnostné stĺpiky (Obrázok 1), doplnené o zábradlie prípadne svetelnú signalizáciu, ktorá sa spustí v prípade, že sa blíži k prechodu električka. Rovnakými pravidlami sa pri prechode riadia aj cyklisti. Tým sa v horizonte 5 rokov zlepšili podmienky, pričom sa budujú samostatné cyklotrasy, ktoré sú oddelené od električkovej dráhy a takisto od cestnej dopravy.

Obrázok 4 Bezpečnostné prvky na električkovej trati (zľava, 1: svetelná signalizácia v chodníku, takisto na náprotivnej strane v úrovni očí dospelého človeka a doplňujúca výstražná značka „Pozor električka" na zábradlí, 2: stĺpiky pred prechodom pre chodcov doplnené o svetelnú výstrahu, 3: stĺpiky oddeľujúce trať od chodníka)(podľa: [2])

2.2 INDIVIDUÁLNA AUTOMOBILOVÁ DOPRAVA (IAD)

Keďže električková doprava je vo veľkej miere vedená stredovým pásom vozovky a oddelená je výškovo prípadne inými bezpečnostnými prvkami, už týmto by sme ju vedeli definovať ako bezpečnú. Bratislava má vytvorenú sieť prechodov pre IAD, ktoré umožňujú križovať električkovú trať s vozovkou. Momentálne je takmer polovica cestných prejazdov riadená semaformi, s absolútnou preferenciou električiek [1].

Preferenciu električiek rozdeľujeme na absolútnu a podmienenú. Absolútna preferencia električiek umožňuje prejazd riadených cestných priecestí bez nutného zastavenia električky. Podmienená preferencia električiek sa používa pri rozsiahlejších križovatkách, aby sa neobmedzila priepustnosť križovatky. Električka zastaví na signál stoj, vyšle impulz do riadenia križovatky, ktorý zastaví všetky smery, okrem smeru, v ktorom premávajú električky (zvyčajne priamy smer). V rámci zohľadnenia brzdnej dráhy električiek a aj v rámci bezpečnosti sa pred svetelné križovatky inštalujú doplnkové signálne svetlá s označením „P“ v žltom obdĺžniku (Obrázok 2), ktoré informujú vodiča električky, aký signál má očakávať na najbližšej svetelne riadenej križovatke [3].

Obrázok 5 Svetelná signalizácia pre vodičov MHD, s doplnkovou tabuľkou „P" informujúca o predzvesti (podľa: [2])

Na neriadených priecestiach s IAD, sú vodiči povinní umožniť električke prejazd a dať jej prednosť ako to vyplýva zo zákona č. 8/2009 Z. z., Zákon o cestnej premávke a o zmene a doplnení niektorých zákonov, konkrétne z §11. Takisto ako pri priechodoch pre chodcov, sa aj vodiči musia presvedčiť, že môžu bezpečne prejsť električkovú trať [4].

2.3 CESTUJÚCI V ELEKTRIČKE

Cestujúci v električke sú rovnako zraniteľní ako chodci. Električky sú vo všeobecnosti skonštruované tak, aby previezli čo najviac cestujúcich a preto je v električke väčší počet cestujúcich, ktorí stoja. V rámci bezpečnosti, sú v električkách madlá, rôzne visiace držiaky a upozornenia, že sa počas jazdy musia cestujúci držať (Obrázok 3). Pri pobyte v zastávke je potrebné sa takisto riadiť nepriamymi pokynmi vodiča, a pokiaľ zaznie zvuková a svetelná výstraha v priestore dverí, cestujúci sú povinní opustiť priestor dverí. Vodiči pri 32-metrových vozidlách a za zníženej viditeľnosti, majú niekedy problém vidieť až na koniec vozidla do priestoru posledných dverí, k čomu im pomáhajú kamery.

Obrázok 6 Upozornenie pre cestujúcich „KEĎ STOJÍTE, DRŽTE SA!" (podľa [2])

2.4 VODIČI ELEKTRIČIEK

Vodiči električiek pracujú z vyvýšeného pracoviska, ktoré im umožňuje lepší rozhľad aj na diaľku. Už kabínu vodiča môžeme považovať za prvok bezpečnosti, keďže je priestranná a vzdialená od čela vozidla. V starších električkách sa nachádza pred karosériou vozidla aj spriahadlo, ktoré slúži na spájanie električiek. V nových električkách je spriahadlo zložené a zakryté prednou maskou. Pri nehodách býva práve spriahadlo ten najrizikovejší prvok, avšak vďaka nemu sa dokážu ochrániť karosérie vozidiel. V kabíne električky ďalej nenájdeme z hľadiska bezpečnosti pás, či airbagy. V novších električkách, ale vieme nájsť obdobné tlačidlo ako v autách. „SOS“ tlačidlo v poslednej dobe musí obsahovať každé auto v rámci bezpečnosti v Európskej Únií. V električkách ale toto tlačidlo zmobilizuje iba políciu a dopravný dispečing dopravného podniku, pričom funguje aj ako

jednosmerná vysielačka, na centrále dopravného dispečingu, počujú všetko čo sa deje v kabíne vodiča, ale nemôžu s ním komunikovať. Používa sa pri fyzickom alebo slovnom útoku na vodiča električky, dobíjania sa do kabína vodiča a slúži na ochranu vodiča [2].

Pre ochranu vozidiel a zvýšenia bezpečnosti sa do predných masiek začal inštalovať antikolízny systém. Systém ochrany funguje v troch krokoch. Najskôr vodiča na potenciálnu prekážku upozorní výstražná ikona na palubnom počítači, po nej nasleduje aj zvukový výstražný signál a nakoniec pokiaľ vodič nereaguje, riadiaci systém vozidla spustí samočinné brzdenie električky. Dokáže identifikovať prekážku na priamej koľaji až na vzdialenosť 80 metrov, pričom sleduje nielen pevné prekážky, ale aj všetky ostatné vozidlá či chodcov. Brzdiť začne prevádzkovou brzdou, aby ideálne zastavil pred prekážkou. Nepreberá 100% zodpovednosť vodiča, ale významne znižuje riziko mimoriadnej udalosti [5].

3 PRÍPRAVA NA PRIDÁVANIE BEZPEČNOSTNÝCH PRVKOV DO OKOLIA TRATE

Pokiaľ chceme pridávať bezpečnostné prvky na trať, musíme v prvom rade analyzovať takzvané „hotspots“, alebo inak miesta, na ktorých často dochádza k nebezpečným situáciám. Pridávanie bezpečnostných prvkov na zastávky, kde nie je veľký pohyb osôb alebo hustota IAD je zanedbateľná, je plytvanie finančných prostriedkov mesta. Dopravné podniky používajú rôzne metódy na identifikovanie týchto „hotspotov“, niektoré si vedú štatistiku dopravných nehôd s chodcami a s IAD, ďalšou metódou je použitie pološtruktúrovaného dotazníka s cieľom zistenia najrizikovejších miest z hľadiska vodičov električiek. Otázky dotazníka ako nástroja pre analýzu potencionálnych rizík môžu byť napríklad tieto:

- Aké nápravné opatrenia boli zavedené?
- Či boli dôsledky opatrení negatívne alebo pozitívne?
- Existujú v električkovej sieti ďalšie miesta, ktoré sú napriek malému počtu nehôd považované za rizikové?
- Boli nejaké miesta „hotspoty“, ale v dnešnej dobe už nie sú? [6]

4 MOŽNOSTI ZVYŠOVANIA BEZPEČNOSTI NA ELEKTRIČKOVÝCH TRATIACH

Riziko v rôznych tvaroch a formách existuje počas celej životnosti električkovej infraštruktúry. Preto sú aktivity zamerané na kontrolu rizika, prípadne jeho obmedzenie, neoddeliteľne spojené po celú dobu funkčnosti. Vyskytujúce sa nebezpečenstvá sa musia vždy posudzovať a v rámci možností aj obmedzovať. V súlade s platnou metodikou sa môže vykonávať riadenie rizík prostredníctvom štyroch etáp: odstránenie alebo zníženie rizika, prenos rizika na iný subjekt, kontrola rizika prostredníctvom systematických opatrení, diagnostiky, pohotovostných plánov a nápravných opatrení. Podstatou riadenia rizík prostredníctvom týchto štyroch etáp sú náklady [7].

V rámci rizík a zároveň aj nápravných opatrení, ktoré spolu súvisia sme vytvorili Tabuľku 1, akú nehodu v respektíve s akým účastníkom nám môžu vzniknúť jednotlivé riziká. Niektoré z nich nepriamo nabádajú aj na nápravné opatrenie, ktoré sa môže vykonať v rámci bezpečnejšej prevádzky električkovej dopravy.

Tabuľka 3 Súhrn rizík spôsobujúcich nehodu s jednotlivými účastníkmi cestnej premávky. Legenda: „X“ – predpoklad vzniku rizika (podľa: [1])

Riziká	Nehody s IAD	Nehody s chodcami a cyklistami	Nehody cestujúcich
Dopravné značenie zobrazujúce oblasť obsluhovanú električkou	X	X	
Efektívnejšie presadzovanie predpisov o parkovaní	X		
Viac križovatiek ovládaných svetelnou signalizáciou	X	X	X
Lepšia informovanosť účastníkov cestnej premávky o prednosti v jazde	X		
Varovné značky ostatným účastníkom cestnej premávky a križovaní električkovej trate	X	X	
Zlepšenie viditeľnosti električiek	X	X	
Budovanie električkových tratí v stredovom pruhu než po krajoch vozovky	X	X	
Odlišné fázy signálov stoj/voľno pre IAD a električky	X		X
Zákaz križovania s električkovou traťou	X		X
Defenzívnejšia jazda električiek	X		X
Oddeľovanie električkovej dopravy od IAD	X		X
Svetelné križovatky riadené električkami (preferencia)	X	X	X
Zvýšenie zorného poľa z kabíny električiek		X	X
Zábrany medzi električkovou traťou a chodníkom pre chodcov		X	
Používanie zvukového signálu počas približovania sa k zastávke alebo prechodu pre chodcov		X	
Odlišné fázy signálov stoj/voľno pre chodcov a električky		X	

Nákup/označenie lístka pred nástupom do električky			**X**
Zvýšenie množstva madiel a držiak v električiek			**X**
Zvýšenie kapacity sedadiel v električke			**X**
Vyhradenie sedadiel pre starších a telesne znevýhodnených cestujúcich			**X**
Zlepšenie systému automatického zatvárania dverí			**X**
Nízkopodlažné električky so zastávkami „hrana k hrane“			**X**

K bezpečnejšej prevádzke môžu prispievať aj samotní jednotlivci, ktorí sa či už priamo alebo nepriamo zúčastňujú cestnej premávky. Preto je potrebné vedieť, ako sa treba správať v blízkosti električkovej trati, aby sme predchádzali jednotlivým nehodám a vytvorili okolo seba bezpečnejšie prostredie dodržiavaním určitých pravidiel.

Chodci:

- Prednostne používať mimoúrovňové prechody (podchody, nadchody).
- Prechádzať električkovú trať na miestach na to určených.
- Presvedčiť sa, či môžu bezpečne prejsť električkovú trať.
- Neprebiehať pred električkou stojacou v zastávke.
- Dať prednosť v jazde električke, ktorá obslúžila zastávku.
- Používať reflexné prvky, osvetlenie.

Cyklisti:

- Využívať prednostne vybudovanú infraštruktúru pre cyklistov.
- V pešej zóne nejazdiť po električkovom páse.
- Pri prechádzaní električkovej trate zosadnúť z bicykla a presvedčiť sa, či môžu prejsť električkovú trať bezpečne.
- Používať reflexné prvky, osvetlenie a takisto ochranné pomôcky – helmu, chrániče.

Vodiči IAD:

- Riadiť sa dopravným značením, umožniť električke prejazd cez križovatku.
- Otáčať sa cez električkovú trať iba na miestach na to určených.
- Pri parkovaní v blízkosti električkovej trati, presvedčiť sa, že časť automobilu nezasahuje do prejazdného profilu trate.

Cestujúci:

- Nedobiehať za električkou.
- Pri čakaní v zastávke, stáť za bezpečnostnou hranicou zastávky.
- Pri zatváraní dverí neotvárať ich manuálne s použitím sily.
- Držať sa v električke počas jazdy.

ZHRNUTIE A ZÁVER

Zvýšenie bezpečnosti na električkových tratiach je kľúčovým aspektom modernizácie dopravnej infraštruktúry a ochrany cestujúcich. Rôzne prístupy môžu pomôcť minimalizovať riziká spojené s prevádzkou električiek a znížiť počet nehôd. Medzi najdôležitejšie možnosti patria modernizácia signalizačných a bezpečnostných systémov, ako aj implementácia pokročilých technológií, ktoré umožňujú detekciu a prevenciu nebezpečných situácií. To môže zahŕňať inštaláciu automatických brzdových systémov, zlepšenie viditeľnosti tratí, lepšiu integráciu dopravných sietí a školenie personálu.

Okrem technických riešení zohráva dôležitú úlohu aj zlepšenie infraštruktúry, ako je výstavba vyhradených pruhov pre električky, oddelenie chodcov a cyklistov od vozidiel a vylepšenie priechodov pre chodcov. Dôležitým faktorom je aj pravidelná údržba a kontrola technického stavu vozidiel, ako aj reakcia na zistené poruchy. Kľúčové je, aby sa tieto opatrenia implementovali v súlade s miestnymi podmienkami a potrebami, pričom neustále monitorovanie a adaptácia na nové výzvy sú nevyhnutné pre efektívnu prevenciu rizík v budúcnosti.

POĎAKOVANIE

Autori tohto príspevku ďakujú Strojníckej fakulte Slovenskej technickej univerzity v Bratislave, grantovej agentúre KEGA projektu číslo 024STU-4/2023 (Budovanie laboratória medicínskej metrológie), grantovej agentúre APVV projektu číslo APVV-21-0216 (Pokročilé matematické a štatistické metódy pre meranie a metrológiu) a grantovej agentúre APVV projektu číslo APVV-21-0195 (Výskum možnosti digitálnej transformácie kontinuálnych dopravných systémov) za ich podporu.

LITERATÚRA

[1] Sagberg F., Sætermo Inger-Anne F. *Traffic safety of tram transport. TØI report 367/1997.* In *Norwegian language.* TOI: https://www.toi.no/getfile.php/138906-1208933888/Publikasjoner/TØI%20rapporter/1997/367-1997/sum-367-97.pdf

[2] *Bratislava*. imhd.sk. [online]. © 2025 [cit. 2025-03-17]. Dostupné z: https://imhd.sk/ba/mhd

[3] Niedzielski, M.A., Goliszek, S. & Górka, A. *Signals, tracks, and trams: public transport signal priority impact on job accessibility over time*. Sci Rep 14, 23459 (2024). https://doi.org/10.1038/s41598-024-74960-x

[4] Zákon č. 8/2009 Z. z. Zákon o cestnej premávke a o zmene a doplnení niektorých zákonov. In: *Zbierka zákonov.* 16.01.2009. Autorský zákon

[5] *Dopravní podnik Ostrava.* Antikolizní systém v tramvajích Stadler. [online]. © 2022 [cit. 2025-04-02]. Dostupné z: https://www.dpo.cz/antikolizak/

[6] *Tramways & urban transit.* Safety management on European tramways. [online]. © 2014 [cit. 2025-03-25]. Dostupné z: http://www.tautonline.com/safety-management-european-tramways/

[7] Szmagliński J., Grulkowski S. and Birr K. *Identification of safety hazards and their sources in tram transport* MATEC Web Conf., 231 (2018) 05008 DOI: https://doi.org/10.1051/matecconf/201823105008

LABORATORNÍ ŘÁD A BEZPEČNOST PRÁCE V LABORATOŘI MEDICÍNSKÉ METROLOGIE

Jan Rybář[1], Jozef Leja[2]

ABSTRAKT

Laboratorní řád a bezpečnost práce v laboratoři medicínské metrologie jsou klíčové pro zajištění kvalitního a bezpečného pracovního prostředí, které je nezbytné pro přesné a spolehlivé měření v oblasti zdravotnictví. Konferenční příspěvek se zaměřuje na stanovení zásad, pravidel a postupů, které musí být dodržovány v laboratořích zaměřených na medicínskou metrologii. Důraz je kladen na prevenci rizik, ochranu zdraví pracovníků a správné používání přístrojů s měřicí funkcí. Důležité je také dodržování požadavků na školení pracovníků, údržbu zařízení, řízení kvality a kontrolu bezpečnostních protokolů. Cílem je nejen zajistit přesnost měření, ale i minimalizovat riziko nehody a zdravotních problémů spojených s fungováním laboratoře.

Klíčová slova:
bezpečnost, laboratoř, medicínská metrologie, řád

ABSTRACT

Laboratory rules and work safety in a medical metrology laboratory are key to ensuring a high-quality and safe working environment, which is necessary for accurate and reliable measurements in the healthcare sector. The conference paper focuses on establishing principles, rules and procedures that must be followed in laboratories focused on medical metrology. Emphasis is placed on risk prevention, worker health protection and the correct use of measuring devices. Compliance with requirements for worker training, equipment maintenance, quality management and safety protocol control is also important. The aim is not only to ensure measurement accuracy, but also to minimize the risk of accidents and health problems associated with the operation of the laboratory.

Key words:
safety, laboratory, medical metrology, order

1 doc. Mgr. Ing. Jan Rybář, PhD., Strojnícka fakulta, Slovenská technická univerzita v Bratislave, Nám. slobody 17, 812 31, Bratislava, +421 949 611 537, jan.rybar@stuba.sk
2 RNDr. Jozef Leja, PhD., Strojnícka fakulta, Slovenská technická univerzita v Bratislave, Nám. slobody 17, 812 31, Bratislava, +421 948 210 850, jozef.leja@stuba.sk

1 ÚVOD DO ŘEŠENÉ PROBLEMATIKY

Práce ve školní laboratoři vyžaduje přesnost, pečlivost a především důsledné dodržování bezpečnostních pravidel. Laboratorní prostředí často zahrnuje práci s elektrickými přístroji, nebo biologickým materiálem, které mohou představovat riziko. Právě proto existuje laboratorní řád – soubor pravidel, jejichž cílem je zajistit bezpečný a efektivní chod laboratorních prací. Dodržování těchto zásad nejen chrání jednotlivce před úrazem, ale zároveň přispívá ke správnosti a věrohodnosti experimentálních výsledků. V této práci se zaměříme na hlavní zásady laboratorního řádu, význam bezpečnosti práce a konkrétní situace, kdy může jejich porušení vést k nežádoucím následkům [1].

Laboratorní pravidla slouží především k ochraně zdraví, bezpečnosti a správnému průběhu práce. V laboratoři totiž hrozí rizika, která v běžném prostředí nehrozí. Bez jasně stanovených pravidel by vznikl zmatek, zvyšovalo by se riziko nehod a výsledky měření by mohly být nespolehlivé. Pomocí laboratorního řádu dokážeme:

- Předcházet chybám způsobeným nepozorností, nebo neznalostí.
- Udržovat pořádek a systém, který je důležitý při práci s přístroji s měřicí funkcí.
- Zvládat krizové situace, protože díky pravidlům každý ví, jak se zachovat např. při úniku látky, nebo úrazu [1].

2 LABORATORNÍ ŘÁD A BEZPEČNOST PRÁCE

Laboratoř medicínské metrologie se zaměřuje na přesné měření a kalibraci měřicích přístrojů a zařízení používaných v oblasti zdravotnictví a medicíny. Cílem laboratoře je zajistit správnost a spolehlivost měření, která jsou klíčová pro diagnostiku, léčbu a monitorování pacientů ve zdravotnickém systému. V laboratoři se studenti učí jak přistupovat ke kalibraci přístrojů, jedná se například o krevní tlakoměry, lékařské teploměry, oční tonometr a jeho metrologické zabezpečení, dále o analyzátory dechu, váhy, jiné měřicí přístroje spojené s lidským zdravím. Laboratoř také podporuje výzkum a vývoj nových měřicích technologií, které přispívají k zajištění vysoké úrovně péče o pacienty [1, 2].

V laboratoři medicínské metrologie je nezbytné mít zavedená pravidla, jako je laboratorní řád, bezpečnostní předpisy a další směrnice z několika klíčových důvodů:

- Zajištění kvality a přesnosti měření: Laboratoř musí provádět přesná měření a kalibrace, které mají přímý vliv na zdraví pacientů. Pravidla pomáhají zajistit, že měření jsou prováděna správně, podle standardizovaných metod a s použitím správně kalibrovaných přístrojů s patřičnou metrologickou návazností.
- Ochrana zdraví a bezpečnosti pracovníků: V laboratoři, kde jsou používány přístroje s měřicí funkcí je důležité mít jasně stanovená bezpečnostní pravidla.

- Soulad s předpisy a normami: Medicínská metrologie musí splňovat normy a legislativní požadavky. Zavedení pravidel zajišťuje, že laboratoř bude v souladu s těmito předpisy, což je klíčové pro její certifikaci, audity a inspekce pro zajištění správného fungování kalibračních, zkušebních a medicínských laboratoří.
- Zajištění transparentnosti a sledovatelnosti: Když jsou v laboratoři zavedená pravidla, je možné sledovat každý krok kalibrace a měření, což zajišťuje auditovatelnost a transparentnost celého procesu. V případě problémů, nebo chyb je možné snadno identifikovat, kde k nim došlo.
- Prevence chyb a zajištění efektivity: Stanovení jasných pravidel pro práci v laboratoři pomáhá předcházet lidským chybám, zvyšuje efektivitu práce a optimalizuje pracovní postupy. To je obzvlášť důležité v prostředí, kde každý detail může ovlivnit výsledky měření.
- Etické a profesionální standardy: Laboratoř medicínské metrologie často pracuje s citlivými daty a zařízeními, která mohou mít vážný dopad na životy lidí. Dodržování etických a profesionálních standardů je proto nezbytné pro zajištění důvěry veřejnosti a pacientů v poskytované služby [2, 3].

3 PREVENCE RIZIK V LABORATOŘI MEDICÍNSKÉ METROLOGIE

Pro prevenci rizik, ochranu zdraví pracovníků/studentů a správné používání přístrojů s měřicí funkcí v laboratoři je možné využít několik nástrojů zaměřených na identifikaci, řízení a minimalizaci rizik. Tyto nástroje (Tabulka 1) pomáhají zajistit, aby byla dodržována bezpečnostní pravidla, přístroje byly správně používány a pracovní prostředí bylo chráněno před nebezpečím.

Tabulka 1 Nástroje prevence rizik v laboratoři (zpracované podle [3-5]).

Nástroj	Popis	Použití
Hodnocení rizik (Risk Assessment)	Systematický proces identifikace a posouzení rizik.	Identifikuje rizika spojená s používáním přístrojů s měřicí funkcí a navrhuje preventivní opatření.
Bezpečnostní školení a instruktáže	Pravidelná školení zaměřená na bezpečné používání přístrojů a ochranu zdraví.	Zajišťuje, že pracovníci mají potřebné dovednosti a znalosti k minimalizaci nebezpečí.
Standardní operační postupy (SOP)	Podrobné pokyny pro používání přístrojů a kalibrace.	Pomáhá zajistit správné používání přístrojů v souladu s bezpečnostními předpisy a normami.
Metoda 5S	Organizace pracovního prostoru pro efektivitu a bezpečnost.	Pomáhá udržet laboratoř v pořádku, což zajišťuje bezpečné

		a efektivní používání přístrojů.
Osobní ochranné prostředky (OOP)	Ochrana pracovníků před nebezpečnými materiály a podmínkami.	Zajišťuje, že pracovníci jsou chráněni před riziky spojenými s používáním přístrojů a materiálů.
Údržba a kalibrace přístrojů	Pravidelná údržba a kalibrace pro zajištění přesnosti přístrojů.	Zajišťuje správnou funkci přístrojů a minimalizuje riziko chybného měření nebo nehod.
Systém řízení kvality (ISO 9001, ISO/IEC 17025)	Mezinárodní standardy pro řízení kvality v laboratořích.	Zajišťuje soulad s normami a správné používání přístrojů v souladu s bezpečnostními předpisy.
Analýza příčin a následků (FMEA)	Identifikace potenciálních chyb a jejich důsledků.	Pomáhá identifikovat slabá místa v procesech a navrhnout opatření k prevenci rizik.
Kontrola environmentálních podmínek	Monitorování teploty, vlhkosti a čistoty vzduchu.	Zajišťuje optimální podmínky pro správnou funkci přístrojů a ochranu pracovníků před nepříznivými vlivy.
Incident Reporting a Follow-Up	Systém hlášení incidentů a jejich analýza.	Umožňuje rychlou reakci na nebezpečné situace a prevenci dalších incidentů v laboratoři.

4 PŘÍKLAD HODNOCENÍ RIZIK PRO BEZKONTAKTNÍ OČNÍ TONOMETR

Hodnocení rizik (Risk Assessment) je systematický proces, jehož cílem je identifikovat potenciální nebezpečí, vyhodnotit jejich pravděpodobnost a závažnost, a následně navrhnout opatření pro minimalizaci těchto rizik v podmínkách laboratoře. Tento proces zahrnuje několik klíčových kroků:

- Identifikace rizik: Identifikace všech potenciálních hrozeb, které mohou ohrozit bezpečnost pracovníků, přesnost měření, nebo provoz přístroje s měřicí funkcí.

- Analýza rizik: Určení pravděpodobnosti, že riziko nastane, a vyhodnocení jeho potenciálního dopadu na zdraví, bezpečnost a kvalitu.

- Hodnocení rizik: Posouzení, zda je riziko přijatelné, nebo zda vyžaduje mitigaci (snížení rizika na akceptovatelnou úroveň).

- Návrh opatření: Navržení a implementace opatření, která minimalizují, nebo eliminují identifikovaná rizika.

- Kontrola a monitorování: Pravidelné provádění kontrol a monitorování účinnosti přijatých opatření [4, 6].

4.1 IDENTIFIKACE, ANALÝZA A HODNOCENÍ RIZIK

Bezkontaktní oční tonometr je přístroj používaný k měření nitroočního tlaku, což je klíčový parametr pro diagnostiku a monitorování glaukomu. Tento přístroj funguje na principu měření odporu oční rohovky na krátký vzduchový impulz, aniž by došlo k fyzickému kontaktu s očima pacienta.

Identifikace rizik
Rizika spojená s používáním bezkontaktního očního tonometru mohou zahrnovat:

- Riziko nesprávného měření, které může být způsobeno nečistotami na senzorech, nesprávným nastavením přístroje, nebo tím, že nebyl přístroj metrologicky zkontrolován.
- Elektrické a mechanické riziko elektrických šoků, nebo mechanických poruch přístroje, které mohou ohrozit pracovníky, nebo pacienty.
- Riziko přenosu infekce může vzniknout i u bezkontaktního přístroje, kde se na senzorech a na okolních částech přístroje mohou zachytit bakterie, nebo viry, které by se mohly přenést mezi pacienty.
- Riziko poranění oka pacienta: Přístroj může být špatně nastaven, nebo může být aplikován příliš vysoký tlak vzduchu, což by mohlo vést k podráždění oka pacienta.
- Riziko neúplného, nebo nesprávného školení personálu, kdy nesprávné používání přístroje může vést k chybám v měření, neadekvátnímu vyhodnocení, nebo poškození přístroje [3, 6, 7].

Analýza rizik
Každé z identifikovaných rizik (Tabulka 2) je vždy posouzeno z hlediska pravděpodobnosti a závažnosti daného rizika:

Tabulka 2 Posouzení identifikovaných rizik (zpracované podle [5-7]).

Riziko	Pravděpodobnost	Závažnost	Celková míra rizika
nesprávného měření	střední	vysoká	vysoká
elektrické a mechanické	nízká	vysoká	střední
přenosu infekce	střední	střední	střední
poranění oka pacienta	nízká	vysoká	střední
neúplného/nesprávného školení personálu	střední	střední	střední

Hodnocení rizik

Na základě analýzy rizik posoudíme, která rizika je třeba okamžitě řešit a která jsou přijatelná.

- Nesprávné měření: Riziko je vysoké, protože nekalibrovaný přístroj může vést k chybám v diagnóze. To musí být prioritně minimalizováno pravidelnou kalibrací (ověřením) přístroje.
- Elektrické a mechanické riziko: I když je pravděpodobnost nízká, závažnost je vysoká. Je nutné provádět pravidelnou údržbu přístroje a zajistit, že pracovníci jsou proškoleni v bezpečnostních opatřeních.
- Přenos infekce: I když je riziko střední, musí se pravidelně provádět dezinfekce přístroje. Pravidelné školení personálu v oblasti hygieny je nutné.
- Poranění oka pacienta: Riziko je nízké, ale je nutné zajistit, že přístroj je správně nastaven a že pracovníci jsou vyškoleni v bezpečném používání.
- Neúplné školení personálu: Riziko je střední a vyžaduje pravidelná školení a aktualizace pro personál, aby se minimalizovaly chyby při použití přístroje [2-4, 8].

4.2 NÁVRH OPATŘENÍ

Na základě hodnocení rizik lze navrhnout následující opatření pro minimalizaci rizik:

- Pravidelná kalibrace (ověření) přístroje – bezkontaktního očního tonometru.
- Údržba přístroje – provádět pravidelné inspekce, zajištění bezpečnosti elektrických komponent a kontrolu mechanických částí.
- Pravidelná dezinfekce přístroje – používat dezinfekční prostředky pro pravidelnou hygienu senzoru a všech částí přístroje, které přicházejí do kontaktu s pacienty.
- Školení personálu – provádět pravidelná školení pro všechny pracovníky v oblasti bezpečného používání přístrojů, kalibrace a hygienických postupů.
- Zajištění správného nastavení přístroje – ujistit se, že přístroj je správně nastaven na každého pacienta a že pracovníci používají přístroj správně [2-4].

4.3 KONTROLA A MONITOROVÁNÍ

Zajistit pravidelný monitoring efektivity přijatých opatření:

- Kontrola kalibrace, a to v pravidelných intervalech provést audit kalibrace bezkontaktního očního tonometru.
- Kontrola údržby a inspekce, minimálně jednou ročně provádět audit údržby a bezpečnostních opatření.
- Zajistit pravidelná školení.

Tato metodika hodnocení rizik pro bezkontaktní oční tonometr v laboratoři medicínské metrologie poskytuje systematický přístup k identifikaci, analýze a mitigaci rizik spojených s tímto přístrojem. Cílem je zajistit bezpečné a efektivní prostředí pro měření nitroočního tlaku a minimalizovat rizika pro pracovníky i pacienty, resp. studenty v podmínkách školní laboratoře [2-4, 8].

SHRNUTÍ A ZÁVĚR

Laboratorní řád a bezpečnost práce jsou klíčovými prvky pro zajištění bezpečného a efektivního provozu v laboratoři medicínské metrologie. Cílem laboratorního řádu je stanovit pravidla, která zajistí správné používání přístrojů, ochranu zdraví pracovníků a pacientů, resp. studentů, a minimalizaci rizik. Součástí těchto pravidel jsou postupy pro údržbu a kalibraci přístrojů, bezpečnostní předpisy, školení personálu a hygienické normy. V laboratoři medicínské metrologie, kde se používají vysoce specializované přístroje, jako je bezkontaktní oční tonometr a jiné výše uvedené, je tedy nutné pečlivě posuzovat potenciální rizika spojená s jejich používáním [5, 7, 8].

V rámci modelového hodnocení rizik bezkontaktního očního tonometru jsme identifikovali klíčová rizika, jako je nesprávné měření kvůli nekalibrovaným přístrojům (chybějící metrologické kontrole), elektrické a mechanické riziko, riziko přenosu infekce, možné poranění oka pacienta a riziko neúplného školení personálu. Na základě analýzy rizik bylo navrženo několik opatření k minimalizaci těchto rizik, včetně pravidelné kalibrace přístrojů, údržby, školení personálu a dezinfekce přístrojů.

Hodnocení rizik a implementace správného laboratorního řádu jsou nezbytné pro zajištění bezpečnosti a kvality práce v laboratoři medicínské metrologie. Pravidelná kontrola a aktualizace těchto opatření, stejně jako školení personálu a údržba přístrojů, jsou klíčovými faktory pro minimalizaci rizik a zajištění přesnosti měření. Zavedení a důsledné dodržování těchto pravidel zvyšuje důvěru v přesnost, spolehlivost a jednotnost prováděných měření, což je nezbytné pro správnou diagnostiku a léčbu, resp. vzdělávání studentů v uvedené oblasti [1-4, 8].

PODĚKOVÁNÍ

Autoři tohoto příspěvku děkují Strojnické fakultě Slovenské technické univerzity v Bratislavě, grantové agentuře KEGA projektu číslo 024STU-4/2023 (Budování laboratoře medicínské metrologie), grantové agentuře APVV projektu číslo APVV-21-0216 (Pokročilé matematické a statistické metody pro měření a metrologii) a grantové agentuře APVV projektu číslo APVV-21-0195 (Výzkum možností digitální transformace kontinuálních dopravních systémů) za jejich podporu.

LITERATURA

[1] DYTRTOVÁ, Radmila; DOBIÁŠOVÁ, Monika a ŠEDIVÝ, Jiří. *Teorie a praxe praktického vyučování: textová studijní opora*. Druhé přepracované vydání. V Praze: Česká zemědělská univerzita, 2023. ISBN 978-80-213-3285-0.

[2] HERCHEL, Radovan; KLANICOVÁ, Alena; ŠINDELÁŘ, Zdeněk a TRÁVNÍČEK, Zdeněk. *Laboratorní technika*. 2. vydání. Olomouc: Vydavatelství Univerzity Palackého, 2023. ISBN 978-80-244-6311-7.

[3] VACHUDOVÁ, Linda. *Kultura bezpečnosti: příručka pro zaměstnavatele*. Praha: Výzkumný ústav bezpečnosti práce, 2024. ISBN 978-80-87676-56-1.

[4] NENADÁL, Jaroslav. *Moderní management jakosti: principy, postupy, metody*. Praha: Management Press, 2008. ISBN 978-80-7261-186-7.

[5] KELEMENOVÁ, Tatiana; DOVICA, Miroslav. *Kalibrácia meradiel*. 1. vydanie. Košice: Technická univerzita v Košiciach, Strojnícka fakulta. Edícia vedeckej a odbornej literatúry, 2016. 232 s. ISBN 978-80-553-3069-3.

[6] PALENČÁR, Jakub; RYBÁŘ, Jan; PALENČÁR, Rudolf; ĎURIŠ, Stanislav; PECIAROVÁ, Zuzana. Measurement on the topcon CT60 non-contact optical tonometer and evaluation of measured data in teaching at university. In *Mechatronics systems and materials 2018*. 1. vyd. Melville: American Institute of Physics. AIP Publishing, 2018, S. 020051-1 - 020051-7. ISBN 978-0-7354-1751-9.

[7] RYBÁŘ, Jan; ĎURIŠ, Stanislav; PAVLÁSEK, Peter; ŠRENKEL, Pavol; CHYTIL, Miroslav. *Měření nitroočního tlaku v oftalmologické praxi*. In *Metrológia a skúšobníctvo*. Roč. 23, č. 1 (2018), s. 8-12. ISSN 1335-2768.

[8] JANKOVÁ, Zuzana. *Řízení rizik v podniku*. Učební texty vysokých škol. Brno: Akademické nakladatelství CERM, 2024. ISBN 978-80-214-6291-5.

DETERMINANTY SPOLEHLIVOSTI STAVEBNÍCH KONSTRUKCÍ SILNIČNÍ KRITICKÉ INFRASTRUKTURY

Ondřej Ryška[1]

ABSTRAKT

Příspěvek se zabývá determinanty spolehlivosti stavebních konstrukcí silničních mostních objektů jakožto prvků silniční kritické infrastruktury. Jsou identifikovány tři klíčové pilíře spolehlivosti: návrhové a posudkové faktory, skutečné provozní zatížení a diagnostika konstrukcí. Zdůrazněn je komplexní přístup ke sledování skutečného stavu mostních objektů a jejich schopnosti odolávat nestandardním provozním situacím.

Klíčová slova:
Mostní objekty, spolehlivost.

ABSTRACT

The paper focuses on factors determining the reliability of road bridge structures as critical road infrastructure elements. Three main reliability aspects are identified: design and assessment criteria, real operational loads, and diagnostics of structures. Special attention is paid to monitoring bridge conditions and their performance during unusual operational situations.

Key words:
Bridge structures, reliability.

1 ÚVOD

Silniční mostní objekty představují strategickou součást dopravní infrastruktury a jsou dlouhodobě vnímány jako klíčový prvek pro zajištění plynulé přepravy a krizového řízení [1,2]. Jejich technický stav a schopnost odolávat mimořádným událostem nabývají zvláštního významu v kontextu požadavků na posílení celkové resilience kritické infrastruktury ve smyslu Směrnice Evropského parlamentu a Rady (EU) 2022/2557. V kontextu rozsáhlých povodní nebo jiných

1 Ing. Ondřej Ryška, Vysoká škola báňská – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství, Lumírova 630/13, 700 30 Ostrava-Výškovice, ondrej.ryska@vsb.cz

závažných naturogenních či antropogenních hrozeb mají silniční mosty rozhodující roli při rychlé evakuaci, transportu humanitární pomoci či při nasazení těžkých záchranných a vojenských prostředků. Spolehlivost jejich stavebních konstrukcí v těchto situacích přímo určují, zda zůstane dopravní koridor nadále provozuschopný, nebo zda dojde k jeho částečnému či úplnému vyřazení. Nedostatečná spolehlivost stěžejních stavebních prvků může při nadstandartním zatížení ve vazbě na specifické scénáře krizového řízení vést k náhlé poruše, a tím i k přerušení dopravní obslužnosti. V takovém případě pak mohou nastat řetězové efekty a mohou se převést na dependentní sektory přímo závislé na provozuschopnosti silniční infrastruktury [3, 4]. Následující text proto detailněji rozebírá stavebně-technické předpoklady spolehlivosti mostních konstrukcí se zvláštním zaměřením na parametry robustnosti ve vztahu k nestandardnímu zatížení.

2 SPOLEHLIVOST MOSTNÍCH KONSTRUKCÍ

Spolehlivost mostních konstrukcí lze charakterizovat jako schopnost daného mostního objektu bezpečně a hospodárně zajišťovat požadovanou funkci po stanovenou dobu. Vychází ze tří vzájemně provázaných pilířů. Prvním pilířem je návrhové a posudkové faktory, které se opírá o normy Eurokódů (například ČSN EN 1991–2) a o související národní předpisy. Ty formulují základní zatěžovací modely a podmínky, jež musí mostní konstrukce při návrhu a ověřovacích procesech splňovat. Druhým pilířem je samotný skutečný zatížení mostní konstrukce, kdy se skutečné zatížení a vlivy prostředí mohou významně lišit od původních návrhových předpokladů [5]. Třetím pilířem je soustavná diagnostika, které umožňují včas odhalit projevy degradace a zamezit jejich progresi [15].

Kromě běžné dopravy působí na mosty též široká škála dalších faktorů, včetně klimatických a geomorfologických vlivů. V některých případech se může jednat o specifické scénáře, jako je přejezd nadměrných a nadrozměrných vozidel či expozice naplaveninám při povodních. Všechny tyto okolnosti se promítají v požadavku identifikace skutečného stavebního stavu konstrukce a posouzení, zda odpovídá potřebným kritériím bezpečnosti a funkčnosti [6]. Nedílnou součástí spolehlivosti je charakterizování skutečných materiálových vlastností (beton, ocel, předpjatý beton) a procesu jejich degradace. Tento proces může zahrnovat korozi, karbonataci, vznik únavových trhlin nebo ztrátu alkalické ochrany výztuže. U stárnoucích mostů je proto nezbytná redukuce návrhové bezpečnostní rezervy, a to je právě nezbytné zohlednit i při stanovení zbývající únosnosti.

2.1 NÁVRHOVÉ A POSUDKOVÉ FAKTORY

Prvním pilířem spolehlivosti mostních konstrukcí je jasně definované a ověřitelné návrhové a posudkové kritérium, které vychází především z norem Eurokódů, konkrétně z ČSN EN 1991–2 [11] pro zatížení mostů dopravou a z doplňujících národních předpisů. Tyto dokumenty formulují základní návrhové podmínky, jež musí mostní konstrukce splňovat z hlediska bezpečnosti, použitelnosti a hospodárnosti po celou dobu plánované životnosti. Základem je

stanovení zatěžovacích modelů odpovídajících nominálnímu zatížení dopravou, avšak i specifické scénáře s potenciálně vyšší hmotnosti či dynamickým účinkům u vybraných kombinací. Normové předpisy kladou důraz nejen na samotnou nosní konstrukci, ale také na spodní stavbu, základy a styčné plochy, které se mohou stát kritickým místem při mimořádných zatíženích. Odchylky od předpokladů, například podcenění lokálních souběhu sil ve styčnících, mohou vést k výskytu trhlin či k urychlené degradaci. Platné předpisy proto zavádějí konzervativní soustavy dílčích součinitelů a mezních stavů, které mají minimalizovat riziko poddimenzování. V případě existujících mostů vstupují do posudkového procesu i doporučení, jež zohledňují možnou degradaci materiálů nebo změny konstrukce provedené během provozu. Cílem je, aby se vypočtená únosnost co nejvíce blížila reálnému stavu, a přitom zůstala zachována dostatečná bezpečnostní rezerva [6]. Tento pilíř vymezuje rámec posuzování a umožňuje systematicky kontrolovat stav mostních objektů, a to včetně případných nestandardních situací, k nimž může dojít při krizovém řízení [1].

2.2 SKUTEČNÉ ZATÍŽENÍ MOSTNÍ KONSTRUKCE

Druhým pilířem spolehlivosti mostní konstrukce je zohlednění reálných provozních a environmentálních podmínek, které mohou výrazně modifikovat původní návrhové předpoklady [5]. Zatímco při standardní dopravní zátěži s homogenní strukturou toku vozidel lze účinky poměrně přesně předvídat. V kontextu silniční kritické infrastruktury je nutné počítat i se specifickými přejezdy nadrozměrných či nadměrných přeprav, jejichž požadavky krizového řízení mohou být rozličné s normovými návrhovými modely [7,8]. Provozní zátěž se navíc vyznačuje dlouhodobým kumulativním působením; opakovaný přejezd těžké dopravy zkracuje únavovou životnost materiálů a může vést ke vzniku únavových trhlin či progresivnímu zeslabení kritických průřezů. Vliv prostředí, včetně teplotních cyklů, chemické expozice nebo zatékání posypových solí, výrazně akceleruje degradaci, čímž se snižuje rezerva materiálových vlastností a zvyšuje riziko křehkého lomu. Pokud realita provozu neodpovídá původním návrhovým mezím, dochází k rychlejší kumulaci poškození, které může vyvolat náhlé omezení únosnosti, a tedy i provozuschopnosti mostní konstrukce. V krizových scénářích, například při povodni či působení unášených naplavenin na pilíře, se problematika dále kombinuje se silným erozním působením, jež může narušit stabilitu spodní stavby [9]. Zohlednění reálného provozu jako druhého pilíře proto vyžaduje průběžné sledování míry zatížení, provozních extrémů i dopadů nestandardních situací, aby bylo možné zjistit, zda skutečné namáhání konstrukce nepřekračuje meze bezpečného návrhu.

2.2 DIAGNOSTIKA MOSTNÍCH KONSTRUKCÍ

Třetím pilířem spolehlivosti mostních konstrukcí je kontinuální a detailní diagnostika, která se opírá o pravidelné i mimořádné prohlídky v kombinaci s pokročilými měřicími technikami [15]. Tyto inspekce zahrnují jak vizuální hodnocení stěžejních konstrukčních prvků, tak specializovaná nedestruktivní zkoušení, například ultrazvukovou detekci trhlin, georadarové mapování

degradovaných zón či monitoring dynamické odezvy. Cílem je včas rozpoznat rané projevy poškození a degradace, například korozi výztuže, vznik trhlin ve vysoce namáhaných úsecích nebo selhávání ložisek, která se mohou stát iniciačními body kolapsu. Na základě takto zjištěného stavebního stavu lze podle potřeby upravit hodnocení zatížitelnosti [6] a případně navrhnout opravné zásahy, jako je výměna kritických dílů, instalace dočasných podpěr či omezení dopravního zatížení. Diagnostika tak představuje nezbytné spojení mezi návrhovou projektovou dokumentací, skutečným zatížením provozem a schopnosti mostních konstrukcí plnit požadavky specifických scénářů v přepravě. V kontextu krizového řízení má klíčový význam fakt, že diagnostika stavebně-technických faktorů usnadňuje rychlou reakci na akutní požadavky na spolehlivost mostních konstrukcí, například při přepravě těžké vojenské techniky nebo rozsáhlé humanitární pomoci, a umožňuje s dostatečnou mírou jistoty rozhodnout, zda lze mostní objekt bez selhání stěžejních funkcí ke konkrétní přepravě využít [1]. Třetí pilíř se tak stává ucelenou zpětnou vazbou pro první dva pilíře, protože poskytuje reálná data o tom, nakolik jsou návrhová a provozní východiska v souladu se skutečným stavem konstrukce a zda je zapotřebí posílit stěžejní dílčí prvky mostní konstrukce pro zvládání nestandardních situací.

3 FAKTORY DETERMINUJÍCÍ SPOLEHLIVOST

Stavebně-technické faktory představují stěžejní východisko pro posouzení vlastností mostních konstrukcí odolávat zatížení v rámci návrhových scénářů, ale rovněž i v mimořádných situacích přesahujících standartní projektové předpoklady. V kontextu silniční kritické infrastruktury se stávají tyto parametry signifikantními, jelikož jejich stavebně-technická úroveň ve vazbě na materiálové vlastnosti přímo na primární úrovni determinují schopnost zachovat funkčnost prvků při nestandartních dopravních či klimatických podmínkách [1]. Konstruktivní uspořádání, vlastnosti materiálů, funkčnost protikorozní ochrany a systematické monitorování degradačních procesů jsou rozhodující faktory, jejichž nedostatečnost může způsobit omezení zatížitelnosti jako signifikantním technickým komponentem spolehlivosti s vazbou na stěžení strukturální stavební prvky jejichž narušením se předpokládá kolaps konstrukce [3, 10].

V prvotní fázi provozu se spolehlivost stavebních konstrukcí opírá o formální návrhové normy definující zatěžovací modely a součinitele bezpečnosti [7, 11]. Tento normativní rámec se však v reálném provozu střetává s podmínkami, které mohou původní návrhové předpoklady překračovat, zejména vlivem vyšší intenzity dopravního zatížení, cyklického namáhání či působení degradačních činitelů [5, 12]. Skutečné stavebně-technické faktory konstrukčních prvků se proto stávají rozhodujícími pro zachování dostatečné rezervy únosnosti a trvanlivosti [13]. S rostoucím stářím konstrukcí narůstá význam včasné detekce degradačních projevů, jako jsou lokální koroze výztuže, trhliny v předpjatém betonu či únavové poškození ocelových prvků, které mohou negativně ovlivnit původní návrhovou robustnost prvků konstrukčního systému [6,14].

Systematické posuzování stavebně-technického stavu pomocí diagnostických metod je proto nezbytné pro kontinuální řízení rizik [1]. Pravidelné inspekční prohlídky, nedestruktivní zkoušky a cílené mapování kritických míst umožňují identifikovat poškození v raných fázích a optimalizovat strategii stavebních zásahů a provozních omezení [10]. V mimořádných situacích vyžadujících přepravu nadměrné nebo nadrozměrné techniky pak pouze skutečná zjištěná data o stavebním stavu umožní rozhodnout, zda a za jakých podmínek lze konstrukci bezpečně využít [8].

Veškeré analýzy spolehlivosti, od návrhových výpočtů po operativní posouzení při mimořádných událostech, se proto soustředí na skutečné stavebně-technické faktory, jež jsou hlavním determinantem zachování požadované úrovně funkčnosti [5]. Kvalita údržby a management těchto faktorů tak rozhoduje o tom, zda lze daný mostní objekt považovat za robustní prvek schopný plnit svou úlohu i v nestandardních provozních podmínkách. Metodická a diagnostická činnost včetně modelování limitních stavů a sledování provozních podmínek tedy sleduje společný cíl: zajistit, aby stavebně-technické faktory efektivně plnily požadavky bezpečnosti, únosnosti a dlouhodobé provozní spolehlivosti [1, 13].

4 ZÁVĚR

Stavebně-technické faktory představují rozhodující determinanty spolehlivosti mostních konstrukcí kritické silniční infrastruktury. Spolehlivost těchto mostních objektů nelze vnímat pouze na základě normativních návrhových předpokladů, ale je nutné nezbytné zohlednit také skutečné zatížení a technický stav konstrukcí. Tři definované pilíře návrhové a posuzovací faktory, reálné provozní zatížení a diagnostika společně formují ucelený rámec, který umožňuje efektivní řízení rizik spojených s provozem mostních konstrukcí a zamezení případným selháním mostních konstrukcí v mimořádných situacích. Stěžením faktorem je zejména schopnost včas identifikovat projevy degradace a zajistit, aby konstrukce splňovala požadavky robustnosti i při nestandardních provozních podmínkách. Výsledky tohoto příspěvku vyzdvihují nezbytnost komplexního přístupu, který integruje stavební diagnostiku, modelování limitních stavů a průběžnou aktualizaci návrhových kritérií v souladu se skutečným stavem a provozními požadavky kritické infrastruktury.

Tento příspěvek byl vytvořen s podporou Vysoké školy báňské – Technické univerzity Ostrava, Fakulty bezpečnostního inženýrství.

LITERATURA

[1] PATRMAN, D., SPLICHALOVA, A., REHAK, D., ONDERKOVA, V. 2019. Factors influencing the performance of critical land transport infrastructure elements. In: Transportation Research Procedia, Vol. 40, p. 1518–1524.

[2] DVORAK, Z., LEITNER, B., REHAK, D. 2019. Critical infrastructure protection specifications in the transport sector. In: MEST Journal, Vol. 7, No. 2, p. 31–40.

[3] REHAK, D., SENOVSKY, P., HROMADA, M., LOVECEK, T. 2019. Complex approach to assessing resilience of critical infrastructure elements. In: International Journal of Critical Infrastructure Protection, Vol. 25, p. 125–138.
[4] LOVECEK, T., STRAKOVA, L., KAMPOVA, K. 2021. Modeling and simulation as tools to increase the protection of critical infrastructure and the sustainability of the provision of essential needs of citizens. In: Sustainability, Vol. 13, No. 11.
[5] DOMING, L.C.P., VINAYKUMAR, C.H. 2021. Comparison of load classification system across the world for interoperability between different countries. In: International Journal of Engineering Research & Technology, Vol. 10, No. 1.
[6] SÝKORA, M., DRAHORÁD, M. 2014. Stanovení dílčích součinitelů pro hodnocení zatížitelnosti existujících mostů. In: Sborník vědeckých prací VŠB-TU Ostrava, Řada stavební, XIV, článek č. 15.
[7] MAŇAS, P., ROTTER, T. 2006. Vyhodnocení zatížitelnosti mostního provizória TMS podle norem NATO. In: Krizové stavy a doprava. Lázně Bohdaneč: Institut Jana Pernera, o.p.s.
[8] COUNCIL OF THE EUROPEAN UNION. 1996. Council Directive 96/53/EC of 25 July 1996. In: Official Journal of the European Communities, L 235, p. 59–75.
[9] HEASLIP, K., LOUISELL, W., COLLURA, J., SERULLE, N.U. 2010. A sketch level method for assessing transportation network resiliency to natural disasters and man-made events. In: 89th Annual Meeting of the Transportation Research Board, Washington, DC.
[10] KHAGHANI, F., JAZIZADEH, F. 2020. mD-Resilience: A multi-dimensional approach for resilience-based performance assessment in urban transportation. In: Sustainability, Vol. 12, No. 12, Article 4879.
[11] EUROCODE. 2005. Eurocode 1: Actions on structures—Part 2: Actions on bridges by traffic (CSN EN 1991-2). Prague: Czech Standards Institute.
[12] SARVI, M. 2011. Modeling and evaluation of freeway operations under critical conditions. In: Australasian Transport Research Forum (ATRF), Adelaide, Australia.
[13] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. 2010. ISO 13822:2010: Bases for design of structures — Assessment of existing structures. 2nd ed.
[14] PAVLÍČEK, F. 2001. Crisis states and transport. Praha: ČVUT. ISBN 80-01-02272-2.
[15] ČSN 73 6221. 1999. Prohlídky mostů. Praha: Český normalizační institut.

VEDE POUŽÍVÁNÍ POHYBOVÝCH SNÍMAČŮ KE SNÍŽENÍ VÝSKYTU MSD NA PRACOVIŠTI?

Karolína Šablaturová[1]

ABSTRAKT

Cieľom tejto práce bolo zhodnotiť, či používanie pohybových snímačov vedie k zníženiu výskytu muskuloskeletálnych ochorení (MSD) na pracovisku. Pozornosť bola zameraná na pracovné prostredie a pokročilé metódy využívajúce senzory, kamery a umelú inteligenciu. Na analýzu boli použité tri vedecké publikácie, ktoré boli vybrané na základe vyhľadávania v databáze Elsevier. Kľúčové slová zahŕňali termíny ako „motion sensor“, „inertial sensor“, „ergonomics“, „MSD“, „WMSD“, „prevention“, „meta-analysis“ a „systematic review“.

Výsledky ukázali, že technológie motion capture zlepšujú kvalitu a kvantitu získaných posturálnych informácií, čo vedie k objektívnejšiemu hodnoteniu rizík. Avšak, žiadna zo štúdií nepreukázala priame zníženie výskytu MSD pri používaní týchto technológií. Diskusia naznačuje, že kvalitnejšie hodnotenie rizík by mohlo potenciálne viesť k zníženiu výskytu MSD, avšak táto hypotéza zatiaľ nie je podložená dátami

Kľúčové slová:
meta-analysis, systematic review, WMSD, MSD

ABSTRACT

The aim of this work was to evaluate whether the use of motion capture technology leads to a reduction in the incidence of musculoskeletal disorders (MSD) in the workplace. The focus was on the work environment and advanced methods using sensors, cameras and artificial intelligence. Three scientific publications were used for the analysis, which were selected based on a search in the Elsevier database. Keywords included terms such as “motion sensor”, “inertial sensor”, “ergonomics”, “MSD”, “WMSD”, “prevention”, “meta-analysis” and “systematic review”.The results showed that motion capture technologies

1 Ing. Karolína Šablaturová, VŠB-TUO FBI, kaolina.sablaturova@vsb.cz

improve the quality and quantity of postural information obtained, which leads to a more objective risk assessment. However, none of the studies demonstrated a direct reduction in the incidence of MSDs with the use of these technologies. The discussion suggests that better quality risk assessment could potentially lead to a reduction in the incidence of MSDs, but this hypothesis is not yet supported by data

Key words:
meta-analysis, systematic review, WMSD, MSD

1 PŘEDSTAVENÍ PROBLEMATIKY

Musculoskeletálním onemocněním (MSD) se rozumí onemocnění svalově kosterní soustavy. Pro rozvoj MSD je potřeba dlouhodobého působení více faktorů na organismus. Jedná se především o nepřiměřenou mechanickou zátěž na jednotlivé muskuloskeletální struktury (špatné provedení pohybu, nevhodná poloha končetin nebo těla). Dalšími faktory mohou být také sociální nebo psychické (stres, diskriminace) a samozřejmě celková organizace práce (směnnost, uspořádání pracoviště nebo zbytečné pohyby a vysoký energetický výdej) [1].

Zaměstnanci v různých odvětvích jsou neustále vystavováni těmto faktorům souvisejícím s rozvojem muskuloskeletálních poruch souvisejících s prací (WRMSD). Nejedná se pouze o Českou republiku, ale také o celou Evropu a jiné industriální země. Proto v roce 2017 EU-OSHA zahájila čtyřletý výzkum týkající se MSD souvisejících s prací. Výzkum sloužil jako podklad pro následující kampaň Zdravé pracoviště 2020-2022. Z výzkumu lze vyčíst, že MSD převažují nad ostatními zdravotními problémy souvisejícími s prací (MSD 60 %, stres, deprese, úzkost 16 %, bolest hlavy 5 % aj.) [1].

Neustále se rozvíjející průmysl klade čím dál více požadavků na bezpečnost práce a hodnocení rizik. V současné době se pro hodnocení rizik souvisejících s WRMSD nejčastěji používají hodnotící metody jako např. RULA, REBA nebo OWAS. Jedná se o systém „papír, tužka“, který je částečně závislý na subjektivním pohledu hodnotitele. Na základě výsledků těchto metod jsou pak navržena nápravná opatření, která mají snížit výskyt rizik na pracovišti.

Do technologie motion capture (snímání pohybu) se zařazuje více systémů. Je to například inerciální snímání, které kombinuje více jednotek. Využívá akcelerometry, gyroskopy, magnetometry či inerciální měrné jednotky (IMU). IMU se skládá z akcelerometru a gyroskopu a měří 3D zrychlení a úhlové rychlosti senzoru s ohledem na gravitaci [2].

2 METODOLOGIE

Důkazy z vědeckých článků na potvrzení či vyvrácení otázky (H0) byly vyhledávány v elektronické databázi Elsevier. Pro vyhledávání vhodných publikací byla nejprve nadefinována klíčová slova, která se následně seskupila tak, aby bylo vyhledávání co nejpřesnější. Řetězec klíčových slov byl sestaven následovně: (“motion sensor“ OR “inertial sensor“ OR „sensor IMU“) AND („ergonomics“ OR „MSD“ OR „WMSD“ OR „prevention“) AND („meta-analysis“ OR „systematic review“). Vyhledávání nebylo omezeno rokem vydání. Do vyhledávání byly zařazeny jen přehledové články. Tento řetězec klíčových slov spolu se zvolenými omezeními vygeneroval 184 výsledků. Ze 184 výsledků bylo vybráno 7 studií na základě nadpisu. Po přečtení abstraktu těchto sedmi studií byly vybrány tři pro zhodnocení jejich plného textu.

3 VÝSLEDKY

První studie (RAHMAN, HASAN, CHOWDHURY, BIN SYED, FARAH; 2024) vyhledávala dostupné publikace týkající se motion capture (snímání pohybu) v průmyslu. 52 z celkem 962 publikací následně podrobovala hloubkové analýze. Z výsledků studie vyplývá, že výzkumná komunita se silně zaměřuje na používání technologie motion capture pro pochopení a zmírnění pracovního rizika především ve stavebním průmyslu. Nejčastějšími sledovanými pohyby bylo zvedání, lezení, výcvik a zdění a využíval se k tomu IMU. Závěrem této publikace je shrnutí výsledků a nastínění budoucích směrů výzkumu v této oblasti jako je např. využití multimodální techniky, zakomponování zpětné vazby v reálném čase či hodnocení komplikovanějších, rychlejších pohybů [3].

V rámci **druhé studie** (SABINO, FERNANDES, CEPEDA; L. NUNES; 2024) byl proveden systematický přehled publikací zaměřujících se na hodnocení rizik pomocí různých systémů snímání těla a analýzu dopadu ergonomických intervencí v prevenci WRMSD ve zdravotnictví. Z celkem 467 publikací bylo vybráno 29, které byly zhodnoceny. Výsledky ukazují, že zdravotničtí pracovníci často zaujímají rizikové pozice z hlediska rozvoje WRMSD. Nejčastějšími rizikovými pohyby byly chirurgické operace nebo manipulace s pacientem a rizikem bylo špatné držení těla a použitá síla. 22 publikací z celkem 26 uvádí jako použitý systém snímání inerciální senzory. V závěru autoři publikace komentují nízký počet zařazených studií a tím omezenou aplikovatelnost systému motion capture v oboru zdravotnictví např. kvůli sterilizačním opatřením. Uvádějí ale, že tyto technologie motion capture odhalují potenciál pro provádění kvalitního hodnocení rizik. Autoři také předpokládají, že získané informace v budoucnu napomohou definovat konkrétní a účinné strategie pro snížení expozice rizikovým faktorům spojeným s WRMSD.

Autoři **třetí studie (**LIM, Sol a D'SOUZA; 2020) se zaměřovali na prozkoumání současného stavu technologií inerciálních systémů snímání pohybu a identifikování potřeb výzkumu a příležitostí pro další využití těchto systémů za účelem měření a zmírnění rizika rozvoje WRMSD. Do přehledu bylo zařazeno 78 publikací z celkem 737 identifikovaných studií. Studie předkládá názor, že hlavním přínosem technologie motion capture je schopnost zvýšit kvalitu a kvantitu získaných posturálních informací a zkvalitnit tak hodnocení oproti pozorovacím metodám.

4 DISKUSE

Ani jedna ze tří zkoumaných studií se nevyjadřuje ke snížení výskytu WRMSD při používání technologie pro snímání pohybu. Studie pouze komentují zkvalitnění hodnocení rizik MSD používáním těchto technologií. Sběr více informací v reálném čase umožňuje objektivnější data pro hodnocení. Kvalitnější hodnocení rizik by mohlo vést ke snížení výskytu MSD při práci a zvýšení produktivity pracovní síly, tato skutečnost ale v současnosti není podložená daty. Je tedy nezbytné pokračovat ve výzkumu a vývoji těchto technologií, aby se maximalizoval jejich potenciál pro zlepšení ergonomických praktik a ochranu zdraví pracovníků.

5 ZÁVĚR

Závěrem lze říct, že studiem dostupné literatury o snímání pohybové aktivity při hodnocení rizik WRMSD nedošlo k vyvrácení ani potvrzení zkoumané hypotézy o snížení rizik MSD při používání pohybových snímačů.

Závěrem také může být přísně nastavená limitace. V případě rozšíření hledání článků o RCTs by výsledek mohl být přesnější.

6 LIMITACE

Přestože technologie MoCap nabízejí objektivní měření biomechanických parametrů a mohou pomoci při identifikaci rizikových pracovních poloh, jejich aplikace stále čelí výzvám, jako je omezení v reálném pracovním prostředí. Jedná se např. o omezení použití technologie ve zdravotnickém prostředí z důvodu hygienických předpisů na operačním sále. Dále současná technologie omezeně hodnotí komplikované a rychlé pohyby.

REFERENCE

[1] Work-related musculoskeletal disorders: prevalence, costs and demographics in the EU. EU OSHA, 2019. ISSN 1831-9343.

[2] LIM, Sol a D'SOUZA, Clive. A narrative review on contemporary and emerging uses of inertial sensing in occupational ergonomics. International Journal of Industrial Ergonomics. 2020, vol. 2020, no. 76, s. 21.

[3] RAHMAN, Md Hadisur; HASAN, Md Rabiul; CHOWDHURY, Nahian Ismail; BIN SYED, Md Asif a FARAH, Mst Ummul. Predictive health analysis in industry 5.0: A scientometric and systematic review of Motion Capture in construction. Digital Engineering. 2024, vol. 2024, no. 1, s. 17.

[4] SABINO, Inˆes; FERNANDES, Maria do Carmo; CEPEDA; L. NUNES, Isabel a TERESA GABRIEL, Ana. Application of wearable technology for the ergonomic risk assessment of healthcare professionals: A systematic literature review. International Journal of Industrial Ergonomics. 2024, vol. 2024, no. 100, s. 14.

ANALÝZA SKORONEHOD A SCÉNÁŘŮ VEDOUCÍCH K VÁŽNÝM PRACOVNÍM ÚRAZŮM

Kristýna Schneiderová[1]

ABSTRAKT

Tato studie se zabývá analýzou skoronehod a scénářů, které mohou vést k vážným pracovním úrazům. Skoronehody, definované jako situace, které téměř vedou k úrazu, představují významný ukazatel potenciálních rizik na pracovišti. Důraz je kladen na faktory, jako jsou nedostatečné školení, nedodržování bezpečnostních předpisů a technické nedostatky zařízení. Výsledky ukazují, že prevence vážných pracovních úrazů může být zlepšena analýzou a intervencí v oblastech, kde dochází ke skoronehodám. Studie rovněž doporučuje implementaci systémů pro hlášení a analýzu skoronehod jako klíčový prvek pro zvýšení bezpečnosti na pracovišti. Cílem je snížit počet vážných úrazů a přispět k celkové kultuře bezpečnosti ve firmách.

KLÍČOVÁ SLOVA:

Skoronehoda, úraz, analýza rizik, bezpečnost práce.

ABSTRACT

This study focuses on the analysis of near-misses and scenarios that can lead to serious workplace accidents. Near-misses, defined as situations that almost result in injury, represent a significant indicator of potential risks in the workplace. Emphasis is placed on factors such as insufficient training, non-compliance with safety regulations, and technical deficiencies of equipment. The results indicate that the prevention of serious workplace injuries can be improved by analyzing and intervening in areas where near-misses occur. The study also recommends the implementation of systems for reporting and analyzing near-misses as a key element in enhancing workplace safety. The goal is to reduce the number of serious injuries and contribute to an overall culture of safety within companies.

KEY WORDS:

Near-miss, injury, risk analysis, workplace safety.

1 Ing. Kristýna Schneiderová, Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, Nad Stráněmi 4511, 760 05 Zlín, kschneiderova@utb.cz

1 ÚVOD

Skoronehoda, označovaná rovněž jako „near miss“ je událost, která by mohla vést k vážnému pracovním úrazu nebo havárii, ale z nějakého důvodu k tomu nedošlo. Tato situace je klíčová pro prevenci nehod, neboť nabízí cenné informace o potenciálních rizicích v pracovním prostředí. Slouží také jako alarmující signál, který může pomoci odhalit slabiny v bezpečnostních opatřeních a pracovních procesech [1].

Definice skoronehody může být formulována následovně: „*Skoronehoda je incident, při němž došlo k nebezpečné situaci, která se blížila ke skutečné nehodě, ale byla odvrácena dříve, než mohla mít vážné následky“* [2].
Tento obrat událostí může zahrnovat široké spektrum situací, od proklouznutí se na kluzkém povrchu, kdy pracovník získal rovnováhu, po technické selhání, které se podařilo včas identifikovat a řešit [2] [3] [4].

Analýza skoronehod je důležitým nástrojem pro zlepšení bezpečnosti na pracovišti. Využití metod jako je například analýza kořenových příčin (Root Cause Analysis) nebo metoda „5 proč“ může pomoci identifikovat faktory, které vedly k těmto situacím. Implementace zjištěných opatření a doporučení z analýz může zásadně přispět k prevenci budoucích pracovních úrazů. Skoronehody, jako indikátory potenciálních problémů, by měly být systematicky zaznamenávány a analyzovány, aby bylo možné neustále zlepšovat pracovní podmínky a udržovat bezpečnost na prvním místě [4] [5] [6].

1.1 TYPY PRACOVNÍCH ÚRAZŮ: DEFINICE VÁŽNÝCH PRACOVNÍCH ÚRAZŮ.

Vážné pracovní úrazy představují situace, kdy dojde k usmrcení pracovníka nebo k těžkému zranění, které vyžaduje okamžitou lékařskou pomoc, zdokumentování a často také hospitalizaci. Tyto úrazy mají zásadní vliv na zdraví pracovníků, jejich zaměstnatelnost a celkovou produktivitu organizace. Je důležité pochopit typy pracovních úrazů, aby bylo možné adekvátně reagovat na jejich prevenci a minimalizaci následků [7].

Podle české legislativy, zejména zákona č. 262/2006 Sb., Zákoníku práce, ve znění pozdějších předpisů, lze vážné pracovní úrazy definovat jako takové, které vedou k *„trvalým následkům na zdraví, ztrátě funkce části těla, ztrátě zraku, ztrátě sluchu, nebo jiné vážné fyzické nebo psychické újmě“* (Česká republika, 2006). Tyto definice reflektují různé typy pracovních úrazů a jsou použitelné v mnoha oborech, včetně průmyslu, stavebnictví, zdravotní péče a dalších [5].

Vážné pracovní úrazy se obvykle klasifikují do několika kategorií:

1. **Úrazy s bezprostředním ohrožením života:** Tyto úrazy mohou zahrnovat vážné pády, popáleniny, elektrické šoky, nebo zranění způsobená strojním

zařízením, kdy je pracovník v ohrožení života [7].

2. Úrazy vedoucí k hospitalizaci: Situace, kdy pracovník potřebuje být hospitalizován kvůli vážnému zranění, jako jsou zlomeniny, vnitřní zranění nebo závažné poranění hlavy [7].

3. Úrazy s trvalými následky: Tyto úrazy mohou mít dlouhodobé zdravotní důsledky, jako je omezení pohyblivosti, chronická bolest nebo psychické poruchy spojené s traumatem [7].

4. Psychosociální úrazy: V této kategorii se nacházejí úrazy související s psychickým zdravím, jako jsou syndrom vyhoření nebo stres, které ovlivňují výkon a zdraví pracovníků [7].

V oblasti hodnocení rizik je důležité při klasifikaci pracovních úrazů zohlednit jak individuální údaje, tak i konkrétní okolnosti události, aby byla zajištěna efektivní prevence a reakce na tyto situace.

Definice vážných pracovních úrazů zahrnuje široké spektrum událostí, které mají potenciál vážně ovlivnit nejen jednotlivce, ale i celé pracoviště. Prevence těchto úrazů by měla být prioritní součástí každého systému řízení bezpečnosti práce [9].

2 LEGISLATIVA

Na Slovensku reguluje oblast bezpečnosti a ochrany zdraví při práci (BOZP) komplexně Zákon č. 124/2006 Z. z., který ukládá zaměstnavatelům povinnost zajistit bezpečné pracovní podmínky. Dále Zákon č. 311/2001 Z. z., Zákonník práce, rovněž zdůrazňuje ochranu zdraví zaměstnanců. V oblasti prevence pracovních úrazů hraje významnou roli Zákon č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia. Nezanedbatelnou součástí legislativy jsou také pravidelné revize elektrických zařízení, jak stanovuje Zákon č. 314/2001 Z.
z. o ochrane pred požiarmi, a technické normy, jako například STN 33 1500, které definují lehoty a metody revizí [18] [20] [21] [22] [23].

Na druhé straně v České republice upravuje obdobné otázky Zákon č. 262/2006 Sb., Zákoník práce, který také stanovuje povinnosti zaměstnavatelů v oblasti BOZP a podobně se věnuje prevenci pracovních úrazů v Zákoně č. 258/2000 Sb. o ochraně veřejného zdraví. I v Česku je důraz kladen na revize technických zařízení, přičemž vyhláška č. 194/2022 Sb. specifikuje bezpečnost práce při používání elektrických zařízení. Technické normy, jako ČSN 33 1500, se rovněž zaměřují na kontrolu a revize elektroinstalací [5] [8] [18] [19]. Lze konstatovat, že ačkoli legislativní rámce obou zemí mají společné cíle v ochraně zdraví a bezpečnosti na pracovištích, specifické požadavky a aplikace se mohou lišit, což odráží místní kontext a potřeby v oblasti BOZP.

3 FAKTORY OVLIVŇUJÍCÍ VZNIK SKORONEHOD

Skoronehody, jsou často výsledkem komplexní interakce různých faktorů. V této kapitole se zaměříme na tři hlavní kategorie které mohou přispět k vzniku těchto nebezpečných situací.

3.1 PSYCHOLOGICKÉ FAKTORY

Psychologické faktory hrají zásadní roli v prevenci pracovních úrazů. Stres a únava jsou dva z nejvýznamnějších faktorů, které mohou negativně ovlivnit rozhodovací procesy pracovníků. Pracovní stres je přímo spojen s nárůstem počtu nehod na pracovišti. Zaměstnanci, kteří trpí dlouhodobým stresem, mají tendenci podceňovat bezpečnostní rizika a častěji se dopouštějí chyb [10].

Dalším kritickým faktorem je nedostatek školení. Zaměstnanci, kteří nejsou dostatečně školeni v prevenci nehod a v používání ochranných pomůcek, jsou vystaveni vyššímu riziku úrazu. Vzdělávání a pravidelné aktualizace znalostí mohou významně ovlivnit schopnost pracovníků identifikovat a reagovat na potenciální nebezpečí [10].

3.2 FYZICKÉ FAKTORY

Fyzické faktory, jako je ergonomie pracovní stanice a zhoršené viditelnosti, také přispívají ke vzniku skoronehod. Ergonomie pracovního prostředí je klíčová pro zajištění pohody a bezpečnosti zaměstnanců. Nevhodně navržené pracovní stanice mohou vést k fyzickému napětí, což zvyšuje pravděpodobnost nehod. Správné uspořádání pracovního místa a používaní ergonomických pomůcek mohou výrazně snížit riziko úrazu [11].

3.3 ORGANIZAČNÍ FAKTORY

Organizační faktory práce hrají klíčovou roli při efektivitě pracovního prostředí. Důležitost koordinace činností a dělby práce mezi jednotlivci slouží k dosažení společného cíle prostřednictvím spolupráce a vzájemné pomoci. Nicméně, organizace čelí výzvám v oblasti motivace a udržení pracovníků, jelikož kvalitní pracovníci nemusí mít vždy naplněné individuální potřeby. Studie ukazují, že špatné organizační klima a vysoká pracovní zátěž mohou vést k negativním důsledkům, jako je zvýšená míra úrazovosti a poranění u personálu. Efektivní komunikace a řízení ze strany managementu jsou nezbytné pro rozvoj organizace a dosažení jejích cílů [12] [13].

4 SCÉNÁŘE VEDOUCÍ K VÁŽNÝM PRACOVNÍM ÚRAZŮM

V mnoha případech bylo možné sledovat několik případů skoronehod,

které pokud by byly zaznamenány a dbalo se na jejich šetření, mohly zaměstnavatele vést k preventivním opatřením. V rámci analyzování pracovního úrazu bylo zjištěno, že v bylo možné úrazu předcházet, pokud by tato evidence byla vedena a dané spotřebiče kontrolovány v rámci měsíčních kontrol. Z rozhovorů se zaměstnanci bylo znát, že se nejednalo o ojedinělý případ, pouze s tím rozdílem, že se tentokrát jednalo o závažnou nehodu a ne pouze o skoronehodu.

Pracovní úrazy s vážnými následky často pramení z kombinace několika rizikových faktorů, které se kumulují a vytvářejí nebezpečné pracovní prostředí. Jedním z hlavních problémů je nedostatečná údržba a revize elektrických zařízení. Používání poškozených spotřebičů, jako například lednice s narušeným kabelem, dramaticky zvyšuje riziko úrazu elektrickým proudem. Absence pravidelných kontrol a revizí pak umožňuje, aby se tyto závady skrytě rozvíjely, a nakonec vyústily v nehodu.

Dalším klíčovým faktorem je nedostatečná pozornost a nedbalost při práci s elektrickými zařízeními. Zaměstnanci, kteří nevěnují dostatečnou pozornost odpojování spotřebičů ze zásuvky, nebo pracují v prostředí s omezenou viditelností poškozených částí zařízení, se vystavují zvýšenému riziku úrazu. V kombinaci s přítomností vody v blízkosti elektrických zařízení se situace stává ještě nebezpečnější. Únik vody, v blízkosti elektrického zařízení, v kombinaci s poškozeným kabelem vytváří ideální podmínky pro úraz elektrickým proudem, zkrat a potenciálně i požár.

V neposlední řadě hraje roli nedostatečné školení a informovanost zaměstnanců. Pokud zaměstnanci nejsou dostatečně proškoleni o bezpečném zacházení s elektrickými zařízeními a o postupech v rizikových situacích, pravděpodobnost úrazu se výrazně zvyšuje. Je klíčové, aby byli zaměstnanci informováni o rizicích spojených s prací s elektrickými zařízeními a o správném postupu v případě závady nebo úniku vody [14] [17].

4.1 POPIS KONKRÉTNÍHO ÚRAZOVÉHO DĚJE

Obrázek 1: Scénář úrazového děje [17]

Dne 31. srpna 2023 v 11:30 došlo k pracovním úrazu ve společnosti XY. Postižena byla zaměstnankyně, na místě byli přítomní svědci.

Při běžném úklidu v pokladní zóně č. 3 zaměstnankyně odsunula chladničku, z níž unikala voda. Při pokusu o odpojení chladničky od elektrické zásuvky došlo k úrazu elektrickým proudem, který byl způsoben poškozeným kabelem chladničky.

Hlavní příčinou nehody bylo poškození elektrického zařízení. Mezi vedlejší příčiny patřily nedostatečná pozornost při vypojování zařízení, špatná viditelnost poškozené části zařízení, nedbalost zaměstnankyně a voda vytékající z chladničky.

Zraněním v důsledku nehody bylo popálení levé ruky zaměstnankyně. Materiální škody zahrnovaly poškozený kabel elektrického zařízení a poškozenou elektrickou zásuvku, přičemž poslední zmiňované poškození bylo zjištěno po nehodě, avšak existovalo již před ní [17].

Analýza tohoto scénáře ukazuje, že prevence vážných pracovních úrazů vyžaduje komplexní přístup, který zahrnuje pravidelnou údržbu a revize zařízení, důkladné školení zaměstnanců a důsledné dodržování bezpečnostních předpisů [14] [17].

4.2 FAKTORY, KTERÉ VEDLY KE VZNIKU PRACOVNÍHO ÚRAZU

V uvedeném scénáři hrály roli různé fyzické faktory, které přispěly k pracovnímu úrazu. Mezi tyto faktory můžeme zařadit na základě šetření úrazu:

1. **Hlavní příčina:**

Poškozené elektrické zařízení: Chladnička měla poškozený kabel, což vedlo k úrazu elektrickým proudem.

2. **Vedlejší příčiny:**

- Nedostatečná pozornost: Zaměstnankyně nevěnovala dostatečnou pozornost při vypojování zařízení.
- Špatná viditelnost: Poškozená část kabelu nebyla snadno viditelná, což ztížilo identifikaci rizika.
- Nedbalost: Došlo k nebezpečnému jednání, když se zaměstnankyně pokusila odpojit chladničku v situaci, kdy unikala voda.
- Voda na podlaze: Unikající voda z chladničky představovala další rizikový faktor, který mohl zhoršit situaci [14].

5 PREVENTIVNÍ OPATŘENÍ

K účinné prevenci skoronehod je důležité komplexní přístupy, které zahrnují identifikaci a analýzu rizik. Je důležité pravidelně provádět hodnocení rizik, aby se identifikovaly potenciální hrozby na pracovišti. Na základě těchto hodnocení by měly být implementovány konkrétní intervence, jako například:

Po nehodě byla nařízena školení zaměstnanců ohledně okolností pracovního úrazu, a došlo k nápravě a odstranění hrozby. Vyšetřování odkrylo, že poškození na elektrickém zařízení a elektrické zásuvce bylo přímou příčinou pracovního úrazu.

1. **Zavedení bezpečnostních protokolů:** Dokumentování a standardizace bezpečnostních postupů pomáhá zaměstnancům lépe pochopit, jak reagovat v krizových situacích. Pravidelné revize a aktualizace těchto protokolů zajišťují, že jsou v souladu s aktuálními normami a nejlepšími praktikami [14].

2. **Školení a vzdělávání:** Školení a vzdělávání zaměstnanců jsou nezbytné pro efektivní prevenci skoronehod. Zaměstnanci by měli být pravidelně školeni v oblasti bezpečnostních opatření, používání ochranných pomůcek a v reakcích na krizové situace. Kvalitní školení je klíčové pro snižování počtu pracovních úrazů a zvyšování celkové bezpečnosti na pracovišti [15] [16].

Preventivní opatření hrají klíčovou roli ve snižování rizika vzniku skoronehod. Kombinace důkladné analýzy rizik, účelových strategických zásahů a kontinuálního školení pracovníků přispívá k vytvoření bezpečnějšího pracovního prostředí [15] [16].

ZÁVĚR

Závěrem lze říct, že kombinace jednotlivých závad vedla k vážným pracovním úrazu. Chyby, které způsobily tuto nehodu bylo možné předvídat a následnému úrazu předcházet. Tento článek se zabýval definicí skoronehod a vážných pracovních úrazů. Na základě konkrétního příkladu bylo ukázáno, že prevence je klíčovým faktorem pro předcházení těchto úrazů a monitorování skoronehod může být dobrým nástrojem pro firmy, aby snížily výskyt vážných pracovních úrazů.

LITERATÚRA

[1] REASON, J. 1997. Managing the Risks of Organizational Accidents. Aldershot: Ashgate. ISBN 978-1840141054.

[2] Výzkumný ústav bezpečnosti práce. Skoronehody. 2024. Dostupné na internete: https://zsbozp.vubp.cz/skoronehody.

[3] MALÝ, S. 2015. Prevence pracovních rizik. Praha: Verlag Dashöfer. ISBN 978-80-87925-04-3.

[4] ČESKO. 2006. Zákon č. 309/2006 Sb., o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci. Sbírka zákonů České republiky.

[5] ČESKO. 2006. Zákon č. 262/2006 Sb., zákoník práce. Sbírka zákonů České republiky.

[6] ČESKO. 2018. Reportování skoronehod a potenciálních incidentů. Česká

asociace petrolejářského průmyslu a obchodu (CAPPO). Dostupné na internete: https://cappo.cz/media/1132/008-2018-reportovani-skoronehod- a-potencialnich-incidentu.pdf.
[7] ČESKO. 2015. Nařízení vlády č. 276/2015 Sb., o odškodňování bolesti a ztížení společenského uplatnění způsobené pracovním úrazem nebo nemocí z povolání. Sbírka zákonů České republiky.
[8] ČESKO. 2000. Zákon č. 258/2000 Sb., Zákon o ochraně veřejného zdraví a o změně některých souvisejících zákonů. Sbírka zákonů České republiky.
[9] SKŘEHOT, P.; BUMBA, J. 2009. Prevence nehod a havárií. Praha: Výzkumný ústav bezpečnosti práce.
[10] VÝZKUMNÝ ÚSTAV BEZPEČNOSTI PRÁCE. Psychologické faktory. 2024. Dostupné na internetu: https://zsbozp.vubp.cz/psychologicke-faktory.
[11] ŠKREHOT, Petr, 2009. Ergonomie pracovních míst a pracovní podmínky zaměstnanců se zdravotním postižením. Výzkumný ústav bezpečnosti práce. ISBN ISBN 978-80-86973-91-3.
[12] MIKULÁŠTÍK, M. Manažerská psychologie. 1. vydání. Praha: Grada, 2013. ISBN 978-80-247-9177-4.
[13] SCHEIN, E. H. 2004. Psychologie organizace. Praha: Grada. ISBN 978- 80-247-1349-6.
[14] Zdroj vlastní – interní podklad.
[15] DITTRICHOVÁ, M. a JUROVÁ, M. 2019. Bezpečnost práce. Praha: Grada. ISBN 978-80-271-0077-4.
[16] DITTRICHOVÁ, M.; JUROVÁ, M. 2019. Bezpečnost práce. Praha: Wolters Kluwer. ISBN 978-80-7623-019-4.
[17] *Záznam o úrazu*. Praha, 2025.
[18] ČESKÁ AGENTURA PRO STANDARDIZACI. ČSN 33 1500, *Elektrotechnické předpisy. Revize elektrických zařízení*. 1991.
[19] ČESKO. 2022. Zákon č. 194/2022 Sb., Nařízení vlády o požadavcích na odbornou způsobilost k výkonu činnosti na elektrických zařízeních a na odbornou způsobilost v elektrotechnice. Sbírka zákonů České republiky.
[20] SLOVENSKO. 2006. Zákon č. 124/2006 Z.z., o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov. Sbírka zákonů Slovenské republiky.
[21] SLOVENSKO. 2001. Zákon č. 311/2001 Z.z., o Zákoník práce. Sbírka zákonů Slovenské republiky
[22] SLOVENSKO. 2007. Zákon č. 355/2007., Zákon o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov. Sbírka zákonů Slovenské republiky
[23] SLOVENSKO. 2001. Zákon č. 314/2001 Z.z., o Zákon o ochrane pred požiarmi. Sbírka zákonů Slovenské republiky.

FIREFIGHTER PERCEPTION OF RISK: APPLICATION OF A QUESTIONNAIRE SURVEY IN THE CZECH REPUBLIC

Patrik Sirotiak[1]

ABSTRAKT

Vnímání rizika hasičem může být jedním z rozhodujících faktorů při hasebních pracích i jiných zásazích. Správný přístup k riziku může zabránit zranění nebo úmrtí hasičů. Zahraniční studie naznačují, že dobrovolní hasiči jsou ochotní přijímat větší míru rizika. Neuvědomují si přitom nebezpečnost situace tak, jako jejich profesionální kolegové. Tyto informace byly získány na základě dotazníkového šetření mezi profesionálními a dobrovolnými hasiči, zejména v oblasti Španělska. Cílem článku je zhodnocení možnosti využití stejné metody dotazníkového šetření v podmínkách české republiky a definování důležitosti psychologického aspektu vnímání rizik na místě mimořádné události.

Kľúčové slová:
Riziko; dotazník; mimořádná událost; vnímání rizika hasičem.

ABSTRACT

Firefighter risk perception may be one of the critical factors in firefighting operations and other emergency interventions. The right attitude to risk can prevent injury or death. Abroad studies suggest that volunteer firefighters are willing to accept a higher degree of risk. They are not as aware of the danger of the situation as their professional colleagues. This information was obtained through a questionnaire survey of professional and volunteer firefighters, particularly in the Spanish region. The aim of this paper is to evaluate the possibility of using the same method in the conditions of the Czech Republic and to define the importance of the psychological aspect of risk perception in emergency interventions.

Key words:
Risk; questionnaire; extraordinary incident; firefighter risk perception.

1 Vysoká škola báňská – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství, Lumírova 630/13, 700 30 Ostrava-Výškovice, patrik.sirotiak@vsb.cz

1 DEFINITION OF A RESCUER - FIREFIGHTER

Each person is unique in their own way. The psychological definition of a good rescuer or firefighter does not depend on his extroverted or introverted behaviour. All the characteristic personality types are found in the fire departments: sanguine, choleric, phlegmatic and melancholic. Also, a specific personality is formed with age. Emotional development, character traits, behaviour patterns, or final intelligence are typical representatives. Fire units intervene every day in various extraordinary incidents. This may be technical assistance in the form of opening enclosed spaces or fighting a large-scale forest fire. Fire brigades (especially intervention commanders of these units) must rely on the quality of work done by their members. Depending on the type and category of the unit, the firefighter must have the necessary knowledge in a certain range, ideally supplemented by experience from similar types of intervention. Equally important are the correct mental state and the perception of potential risk by each individual firefighter at the place of the intervention. Psychological state and risk perception at the site of intervention are attributes that are usually quite unclear for intervening firefighters. The method of carrying out rescue and liquidation works at the extraordinary incident is mainly controlled by the instructions of the commander. However, the specified activities are subsequently carried out by individual persons [1].

1.1 PROFESSIONAL FIREFIGHTERS VERSUS VOLUNTEER FIREFIGHTERS

Although professional and volunteer firefighters perform practically the same activities in the Czech Republic, the demands on their mental resistance, health, physical ability, or knowledge differ considerably. As part of the recruitment process for the Czech Republic Fire Rescue Service, candidates undergo a psychological diagnosis and a psychiatric examination. The aim is, among other things, to exclude mentally unstable persons and persons with low self-preservation instincts. This is fixed by legislation in the Act on the service of members of the security forces. Subsequent legislation also provides a summary of the characteristics to be verified and the methods of verifying them in the recruitment process. The psychological diagnosis of candidates for the firefighter position is usually carried out during one day in the range of 5 to 8 hours, depending on the number of candidates and the speed of completion of the submitted tests. According to some sources, the success rate of this diagnosis is approximately 68,75 % [2, 3, 4].

Members of the Czech Republic Fire Brigade should be able to cope with stressful impulses and long-term stress in extraordinary incidents based on psychological diagnostics. However, the level of these qualities is quite unclear for volunteer firefighters, although professional firefighters are often involved in volunteer units. There are no psychological resilience requirements for volunteer firefighters of all categories. Firefighters are exposed to many risks in

the performance of their job. In extreme cases, their own lives may depend on the level of risk perception at the intervention. The risk perception and level of exposure to risk are always slightly unclear for professional firefighters, while for volunteer firefighters, unless they are also professional firefighters, the ability to perceive risk and the level of exposure to risk are completely unclear. Foreign studies suggest that the possibility of choice in volunteer fire protection units (each volunteer firefighter can choose whether to go on a rescue) results in a reduced level of risk perception at the scene and a lower instinct for self-preservation in crisis situations [5, 6, 7].

2 REPLICATION OF FOREIGN RESEARCH

In the area of mental health, perception of stress and risk at the intervention place, progress has been very slow, especially for volunteer units. A proper mental set-up with a focus on risk perception is an important aspect for the correct and safe execution of rescue and recovery work.

Firefighter risk perception has been addressed in several studies. Research has been carried out on professional and volunteer firefighters mainly in the Spanish region. On a minor scale also in Argentina, Chile and Ecuador. The basic idea is to define a psychometric paradigm of overestimating or underestimating the importance of risk in a specific area. By replicating the questionnaire from previous research, focusing on specific aspects of risk perception, self-preservation, level of risk exposure and other psychological states related to the performance of a firefighter at the intervention place, individual aspects can be effectively assessed using statistical methods. The assessed differences can lead to changes in additional training or the implementation of courses for units and can thus prevent injuries or deaths of firefighters at the intervention. It was decided to replicate the questionnaire survey in the Czech Republic.

The original questionnaire consists of an introduction that contains demographic information that each participant must complete. For the questionnaire survey, nine basic questions were established to define the psychometric paradigm of the firefighter's perception of risk at the scene of an emergency. Additional questions include global risk perception and stress perception during the intervention. These questions involve qualitative and quantitative levels of research and include the following areas [5, 6, 7]:

Q1 - knowledge on occupational safety,
Q2 - supervisor's knowledge of health and safety,
Q3 - fear,
Q4 - fear of personal vulnerability,
Q5 - seriousness of consequences,
Q6 - perception of control over destiny,
Q7 - control of risk,

Q8 - potential of disaster/risk,
Q9 - delay of consequences,
Q10 - global risk perception,
Q11 - perception of stress,
Q12 - optional question (stress management techniques).

The results of the questionnaire were statistically processed. The best method for the quantitative part of the research is the use of the T-test. This can be used if the values meet the assumptions of normality (approximately normal distribution of data) and both groups have similar variances. Chi-square analysis is used for the qualitative part of the research. This test can be used to test the dependence between categorical data. But can we use the same questionnaire for firefighters in the Czech Republic? [5, 6, 7]

3 COMPARISON OF THE FIRE PROTECTION SYSTEM IN SPAIN AND THE CZECH REPUBLIC

This chapter examines the differences between the fire protection system in the Czech Republic and in Spain. It will focus on the differences between professional and volunteer firefighters in predefined areas. These areas have the greatest influence on the differences in the type of recruits between professional and volunteer firefighters. Areas include categories of fire protection units, admission requirements, psychological screening, unit establishment and deployment.

3.1 CATEGORIES AND TYPES OF FIRE PROTECTION UNITS

The original questionnaire only included the option to be classified as a professional or volunteer firefighter. In the Czech Republic, fire protection units are divided into six categories according to the Fire Protection Act: FRU I. - professional units of the FRS of the region, FRU II., III. – volunteer units of the VFD of municipalities, FRU IV - professional units of the FRS of companies, FRU V. - volunteer units of the VFD of municipalities, FRU VI. - volunteer units of the VFD of companies.

Fire protection units in Spain are not divided into categories as in the Czech Republic. Voluntary units form a separate category, professional units have their own classification. Municipal Fire Departments - Operates in municipalities with more than 20,000 inhabitants. Provincial and Consortium Fire Departments - Provide services in regions where municipalities cannot afford their own fire department. Autonomous Community Firefighters - operate in areas not covered by municipal fire departments and address specific regional needs. Forest Firefighters - specialize in preventing and fighting fires in natural areas. Military and Airport Firefighters - provide security at military installations and civilian airports. Private Firefighters - professionals hired by companies to

provide fire safety at specific facilities. Volunteer firefighters - citizens who supplement the work of official departments [8].

Although the distribution of units in Spain is different, they are practically the same categories of units that can be found in the Czech Republic. The approach to risk may depend not only on the basic division between professional and volunteer firefighters, but also on the specific unit. Although there is more than one category of professional firefighters in Spain, this is not included in the original questionnaire. Therefore, based on the information contained in this chapter, the original questionnaire will be modified. By adding an additional question with the option to select a specific category of unit, more accurate data can be obtained in the statistical evaluation.

3.2 REQUIREMENTS FOR ADMISSION TO THE FIRE DEPARTMENT

In the Czech Republic, there are uniform requirements for future members of the Fire Rescue Service. There are basic admission conditions for professional company firefighters and members of the municipal Fire Departments. However, the requirements for admission to voluntary or company firefighters are lower and provide more freedom in decision making and setting admission conditions. Some of the conditions vary depending on whether the person is a professional firefighter of the company's fire department or the regional fire department. Company firefighters have simpler conditions. An overview of the conditions is given in Table 1. [4, 9].

Table 5 Requirements in the Czech Republic

Requirement	Professional firefighter	Volunteer firefighter
Nationality	citizen of the Czech Rep.	X
Age	18+	18+
Education	Secondary - matriculation	X
Driving license	X (but mostly gr. B)	X
Physical tests	✓	X
Psychological tests	✓	X
Medical fitness	✓	✓
Entry course	✓ (600/120 hours)	✓ (40 hours)
Annual training	✓ (list of topics)	✓ (40 hours)

In Spain, the requirements may vary according to the autonomous communities, but the basic requirements are the same for all regions. The admission conditions to volunteer fire departments are adjusted depending on the specific region or department. In general, the requirements in Spain are very variable depending on the region. The basic requirements for firefighters in Spain are shown in Table 2. [10, 11].

Table 2 Requirements in Spain

Requirement	Professional firefighter	Volunteer firefighter
Nationality	citizen of Spain.	X
Age	18+ (depending on region)	18+ (depending on region)
Education	secondary school	X
Driving license	group B	X
Physical tests	✓	X
Psychological tests	✓	X
Medical fitness	✓	✓
Entry course	✓ (according to region)	✓ (according to region)
Annual training	✓ (list of topics)	✓ (according to region)

According to the provided information, there are no major differences in the selected requirements. Based on this chapter, the questionnaire can be applied without modification in terms of admission conditions.

3.3 PSYCHOLOGICAL SCREENING

Psychological tests for firefighter candidates are a key part of the selection process, as they assess the candidates' personal suitability for this demanding profession. In the Czech Republic, psychological tests can be divided into 3 parts: a performance part, a personality part and an interview with a psychologist. The performance part includes tests of attention, speed and accuracy of reactions and tests of intellect. The personality part includes questionnaires focused on the candidate's character, his behaviour in stressful situations and his overall personality structure. The third part includes a discussion of personal history, motivation and other relevant topics. The psychologist then evaluates all the tests and decides on eligibility [4, 9].

In Spain, the requirements for psychological tests may vary depending on the autonomous communities and particular fire departments. In general, the selection procedure includes psychological tests and personality tests. Psychological tests assess cognitive and psychological abilities such as logical thinking, memory and attention. Personality tests assess personality traits and suitability for the job of firefighter. The exact information on the duration of these tests and the specific results required is not uniform throughout Spain and may vary by region [11].

According to the above information, the psychological tests in the Czech Republic and Spain can be assessed as similar in content. According to this chapter, the questionnaire can be used without additional modifications.

3.4 ESTABLISHMENT OF FIRE PROTECTION UNITS AND THEIR DEPLOYMENT

In the Czech Republic, every municipality must have a fire protection unit. However, it is possible to set up a shared unit in cooperation with another municipality and share the costs of its operation. Fire protection is organised based on area coverage, which is a term referring to the targeted distribution of fire protection units on the territory of the region and the territory of the capital city of Prague. Area coverage regulates the number of forces and resources and the time of arrival at the site of an incident [12, 13].

In Spain there is not a uniform national system for the establishment and categorisation of fire units as we know in the Czech Republic. The organisation of fire protection is decentralised and governed at the level of the individual autonomous communities (regions). Some regions have a high level of fire protection, e.g., Catalonia, while rely more on help from their surroundings. Professional firefighters are set up by provinces, cities of more than 20 000 inhabitants or regions. Volunteer fire departments are not established by statute or law. The establishment of fire protection units is more based on the specific needs of each area, regions and cities [10, 14].

Fire protection units are established in different ways, but there is no need to modify or supplement individual questions. These are still professional and voluntary firefighters of similar types.

4 FINAL FORM OF THE QUESTIONNAIRE FOR THE CONDITIONS OF THE CZECH REPUBLIC

Based on a previous survey of selected fire protection areas, modifications were made to the final version of the questionnaire. Specific topics and questions were consulted with the psychological service of the Czech Republic Fire Rescue Service and other people, especially from the field of fire protection. The questionnaire is supplemented by an introductory prologue that defines the purpose of the survey and asks for subjective completion of the questionnaire. This was not included in the original questionnaires. In addition, firefighters completing the questionnaire must choose between the functions of firefighter, firefighter-driver, commander and indicate the category of their fire protection unit. The questions are always accompanied by a graphic scale with marked numerical answers from 1 to 5. The questions have been translated and adapted to make them easier to understand for people in the Czech Republic. Some of the questions were not easily understandable once translated into Czech. An emphasis has been placed on keeping the meaning of the sentence the same. The questionnaire is currently being sent to Fire Rescue Services in the Czech Republic and at the time of writing has over 170 participants.

LITERATÚRA

[1] ŠVÁB, Svatoslav. Psychologie práce pro nováčky, hasiče-záchranáře, ale nejen pro ně. Ostrava: SPBI, 2006. ISBN 80-86634-84-1.

[2] Zákon č. 361/2003 Sb.: o služebním poměru příslušníků bezpečnostních sborů. In: *Sbírka zákonů*. 2003.

[3] HURDÁLKOVÁ, Anna. Úspěšnost potenciálních uchazečů u přijímacích fyzických testů HZS a PČR. Olomouc, 2023. bakalářská práce (Bc.). UNIVERZITA PALACKÉHO V OLOMOUCI. Fakulta tělesné kultury

[4] GŘ HZS ČR. *Podmínky přijetí do služebního poměru a další informace*. Online. HZS ČR. C2024. In: https://www.hzscr.cz/clanek/podminky-prijeti-do-sluzebniho-pomeru-a-dalsi-informace.aspx?q=Y2hudW09Mg%3d%3d.

[5] RODRÍGUEZ-GARZÓN, Ignacio, Myriam MARTÍNEZ-FIESTAS, Adrian DARMOHRAJ, Antonio DELGADO-PADIAL a Ruben CHUMPITAZ. Voluntary and involuntary risk acceptance: A case study of firefighters. Safety Science [online]. 2021, 142. ISSN 09257535. In: doi:10.1016/j.ssci.2021.105394

[6] MARTÍNEZ-FIESTAS, Myriam, Ignacio RODRÍGUEZ-GARZÓN a Antonio DELGADO-PADIAL. Firefighter perception of risk: A multinational analysis. Safety Science [online]. 2020, 123. ISSN 09257535. In: doi:10.1016/j.ssci.2019.104545

[7] RODRÍGUEZ-GARZÓN, Ignacio; MARTÍNEZ-FIESTAS, Myriam; DELGADO-PADIAL, Antonio a LUCAS-RUIZ, Valeriano. Perception of Occupational Risk of Firefighters in Quito (Ecuador). Online. Fire Technology. 2016, s. 753-773. ISSN 0015-2684. In: https://doi.org/10.1007/s10694-015-0494-x.

[8] Classification and types of firefighters in Spain. Online. Incipresa. 2024. In: www.incipresa.com/en/classification-and-types-of-firefighters-in-spain.

[9] Psychologická diagnostika pro potřeby HZS Středočeského kraje. Online. HZS Středočeského kraje. In: https://hzscr.gov.cz/clanek/psychologicka-diagnostika-pro-potreby-hzs-stredoceskeho-kraje.

[10] *The Firefighter Exams in Spain: Requirements, Tests and Advices*. Online. Incipresa. 2024. In: https://www.incipresa.com/en/firefighter-competitions-in-spain-requirements-tests-advices/.

[11] BERGES, Alfredo; FERNÁNDEZ-DEL-RÍO, Elena a RAMOS-VILLAGRASA, Pedro J. The Prediction of Training Proficiency in Firefighters: A Study of Predictive Validity in Spain. Online. *Revista de Psicología del Trabajo y de las Organizaciones*. 2018, pub, no. 1, s. 1-13. ISSN 1576-5962. In: https://doi.org/10.5093/jwop2018a2.

[12] Zákon 133/1985 Sb. o požární ochraně. In: *Sbírka zákonů*. 1985.

[13] Vyhláška 247/2001 Sb.: o organizaci a činnosti jednotek požární ochrany. In: Sbírka zákonů. 2001.

[14] Audícana Amenábar, M. G. de. Analysis of Fire Services Coverage in Spain 2018. DYNA. Publicaciones DYNA.

VYUŽITIE VNÚTORNÝCH POLOHOVACÍCH SYSTÉMOV V RÁMCI INFORMAČNEJ BEZPEČNOSTI

Erika Skýpalová[1], Martin Boroš[2]

ABSTRAKT

Lokalizačné služby založené na určovaní polohy vo vnútorných priestoroch sú v súčasnosti pomerne dobre známe a široko využívané v rôznych sférach života ľudí – školstvo, zdravotníctvo, obchod, doprava či priemysel a sú súčasťou infraštruktúry moderných budov. Vnútorné polohovacie systémy je možné využiť i pre aplikáciu v rámci informačnej bezpečnosti. Informácie o polohe sú užitočné pri riadení a správe informačných aktív. Poznanie polohy osôb umožňuje eliminovať neoprávnené prístupy do chránených priestorov, ako sú serverovne či priestory, v ktorých sa nachádzajú chránené informačné aktíva. Okrem pohybu a polohy osôb v priestore je možné sledovať i pohyb hardvérových komponentov informačných systémov, ako sú servery, úložiská, sieťová infraštruktúra či ďalšie prvky informačno-komunikačných technológií. Článok pojednáva o výsledkoch testovania vnútorného polohovacieho systému na báze nízkoenergetickej technológie Bluetooth zameraného na skúmanie spoľahlivosti 2 rôznych typov prijímacích zariadení na účely lokalizácie osôb a entít vo vnútri budov.

Kľúčové slová:
Vnútorné polohovacie systémy, určovanie polohy, informačné systémy, informačné aktíva, informačná bezpečnosť.

ABSTRACT

Indoor location-based services are now quite well known and widely used in various spheres of people's lives - education, healthcare, retail, transport or industry, and are part of the infrastructure of modern buildings. Indoor positioning systems can also be used for information security applications. Location information is useful in the management and administration of

1 Ing. Erika Skýpalová, Fakulta bezpečnostného inžinierstva, Univerzitná 8215/1, 010 26 Žilina, 041 513 6670, erika.skypalova@uniza.sk

2 Ing. Martin Boroš, PhD., Fakulta bezpečnostného inžinierstva, Univerzitná 8215/1, 010 26 Žilina, 041 513 6610, martin.boros@uniza.sk

information assets. Knowing the location of people allows eliminating unauthorized access to protected areas such as server rooms or areas where protected information assets are located. In addition to the movement and location of people in the space, it is also possible to monitor the movement of hardware components of information systems, such as servers, storage, network infrastructure or other components of information and communication technologies. This paper discusses the results of testing an indoor positioning system based on Bluetooth Low Energy, aimed at investigating the reliability of 2 different types of receiving devices for the purpose of locating people and entities inside buildings.

Key words:
Indoor positioning systems, positioning, information systems, information assets, information security.

1 VNÚTORNÉ POLOHOVACIE SYSTÉMY

Vnútorné polohovacie systémy umožňujú lokalizáciu osôb alebo predmetov v uzavretom priestore. História určovania polohy vo vnútri objektov siaha do začiatku milénia, keď boli vyvinuté systémy ako RADAR, Active Badge a Where2Project. Tieto sústavy využívali technológie Wi-Fi, ultrazvuk, Bluetooth a infračervené technológie. Vnútorné polohovacie systémy využívajú na určenie vnútornej polohy rôzne snímače. Informácie o polohe daného cieľa sa odosielajú do centrálneho systému, ktorý sa môže aplikovať na navigáciu, informovanie alebo napríklad monitorovanie zdrojov. Vnútorný polohovací systém trpí problémami obmedzenej presnosti v dôsledku útlmu signálu, rušenia, viaccestného šírenia a zložitosti prostredia [1], [2].

Za posledné desaťročia došlo k technologickému pokroku v oblasti riešení pre vonkajšie umiestnenie. Technológia GPS umožňuje ľuďom dostať sa na miesta, ktoré nikdy predtým nenavštívili. Systémy tiež umožňujú osobám nepretržite zdieľať svoju polohu s rodinnými príslušníkmi, priateľmi alebo v prípade potreby včasnej lokalizácie záchrannými službami [3].

Bezdrôtová lokálna sieť (WLAN), ZigBee, ultraširoké pásmo (UWB), komunikácia viditeľným svetlom (VLC) a nízkoenergetická technológia Bluetooth (BLE) predstavujú bezdrôtové polohovacie systémy vo vnútri budov využívajúce bezdrôtové komunikačné technológie [4], [5].

1.1 NÍZKOENERGETICKÁ TECHNOLÓGIA BLUETOOTH BEACONOV

Nízkoenergetická technológia Bluetooth, známa ako Bluetooth Smart, sa vyznačuje nízkymi obstarávacími nákladmi, energetickou účinnosťou a jednoduchou implementáciou. Cieľom tejto technológie je predĺžiť životnosť batériou napájaných zariadení tým, že umožňuje krátke dátové prenosy

namiesto nepretržitých dátových tokov, ktoré spôsobujú rýchlejšie vybíjanie batérie [6].

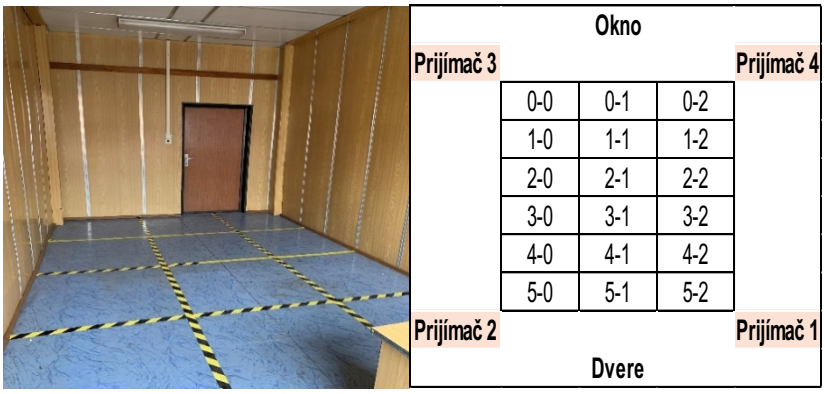
Patrí medzi bezdrôtové rádiové technológie krátkeho dosahu a je vhodná pre nízkoenergetické senzory napájané malými mincovými batériami. Dosah signálu môže byť ovplyvnený rôznymi faktormi prostredia, čo môže viesť k nepresným výsledkom pri výpočte vzdialenosti pomocou techniky RSSI [7], [8], [9]. Formát údajov BLE obsahuje 4 hlavné typy informácií, a to UUID, Major, Minor a Tx-power [10].

Indikátor sily prijatého signálu (RSSI) je algoritmus na určovanie polohy v uzavretom priestore. RSSI sa používa na meranie vzdialenosti medzi vysielačmi a prijímačmi. Je založený na energetickej sile prijatého signálu na určenie vzdialenosti. Čím je vzdialenosť väčšia, tým je sila signálu slabšia. Na silu energie majú negatívny vplyv prekážky, ktoré ovplyvňujú presnosť určenia vzdialenosti [11], [12].

2 METODOLÓGIA

Prototyp vnútorného polohovacieho systému pozostáva z vysielacích a prijímacích zariadení. Vysielacími zariadeniami sú Bluetooth beacony Gigaset G-Tag Red. Prijímacie zariadenia sú mikropočítače Raspberry Pi Zero. Je možné použiť iné zariadenia, napríklad v prípade prijímacích zariadení to môžu byť mikrokontroléry z rady Arduino. Avšak bolo realizované experimentálne testovanie v laboratórnych podmienkach, ktorého cieľom bolo porovnať prijímaciu schopnosť 2 typov prijímacích zariadení z hľadiska ich vplyvu na kvalitu sily prijímaného signálu.

Na účely testovania bolo vybrané 1 vysielacie zariadenie a 2 rôzne typy prijímacích zariadení. Vysielacím zariadením bol beacon Gigaset G-Tag Red. Ako prijímacie zariadenia boli použité 4 mikropočítače Raspberry Pi Zero s operačným systémom Raspbian a tiež 4 zariadenia Arduino Nano IoT. Testovanie sa uskutočnilo v podmienkach uzavretého priestoru s rozmermi 3 x 5,5 m. Pred samotným testovaním bolo potrebné pripraviť podmienky na testovanie v danom priestore. Testovacia miestnosť bola rozdelená na 18



Obrázok 1 Príprava testovacieho priestoru a schéma rozčlenenia priestoru

sektorov. 15 sektorov malo rozmery 1 x 1 m, zatiaľ čo sektory 0-0, 0-1 a 0-2 mali rozmery 0,5 x 1 m. Rozdelenie priestoru a označenie. Rozčlenenie priestoru a označenie jednotlivých sektorov je znázornené na *Obrázku 1.* V každom rohu miestnosti boli umiestnené mikropočítače Raspberry Pi Zero a Arduino Nano IoT, ktoré prijímali údaje prenášané Bluetooth beaconom a potom ich odosielali na server. Jednotlivé rohy miestnosti predstavujú miesta umiestnenia prijímacích zariadení. Prijímacie zariadenia umiestnené v 4 bodoch miestnosti boli nainštalované vo výške 1,8 m. Beacon Gigaset G-Tag Red bol umiestnený v strede sektorov 2-0, 2-1 a 2-2. Podmienkou testovania bol pevne stanovený časový interval zberu údajov. Hodnoty RSSI sa zaznamenávali počas 5 minút v každom sektore. Ďalšou podmienkou bolo určenie maximálneho počtu spracovaných údajov. Na účely výpočtov sa použilo maximálne 1 000 hodnôt RSSI pre každé prijímacie zariadenie. Potom sa vypočítali maximálne, minimálne a priemerné hodnoty beaconu Gigaset G-Tag Red vo vybraných sektoroch a pre každé prijímacie zariadenie.

3 VÝSLEDKY

Hodnoty RSSI získané z vykonaných meraní boli uložené na serveri počas 5 minút, pričom sa pracovalo s maximálne 1000 hodnotami RSSI prijatými každým prijímacím zariadením. V Tab. 4.1 je uvedený počet hodnôt RSSI prijatých zariadeniami Raspberry Pi Zero a Arduino Nano IoT v každom sektore.

Tabuľka 1 Počet hodnôt RSSI prijatých zariadeniami Raspberry Pi Zero a Arduino Nano IoT

Sektor	Raspberry Pi Zero	Arduino Nano IoT
2-0	1123	348
2-1	1097	332
2-2	1185	374

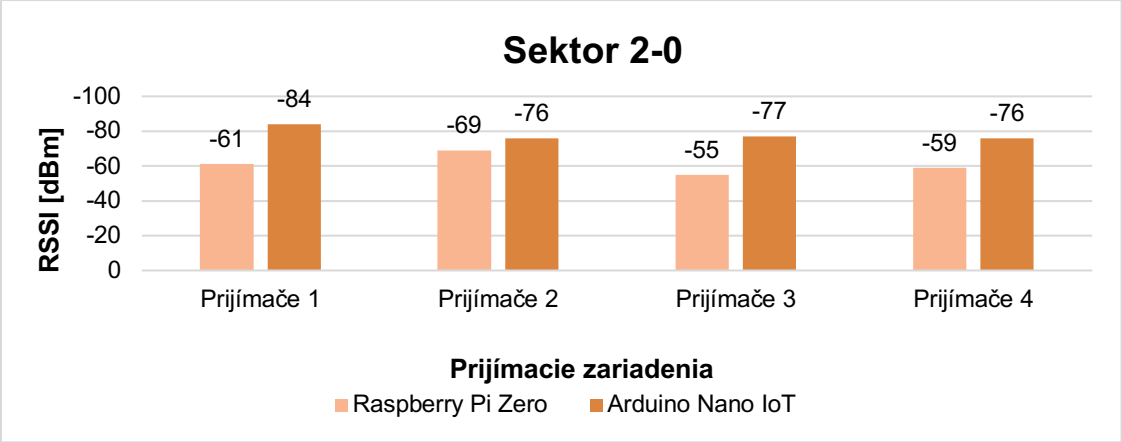
Následne sa získané údaje rozdelili podľa typu prijímacích zariadení a ich umiestnenia v priestore. Po rozdelení údajov boli vypočítané maximálne, minimálne a priemerné hodnoty RSSI. V Tab. 4.2 a 4.3 sú uvedené výpočty hodnôt RSSI pre každé prijímacie zariadenie umiestnené vo výške 1,8 m.

Tabuľka 2 Maximálne, minimálne a priemerné hodnoty RSSI [dBm] prijímačov Raspberry Pi Zero

Prijímacie zariadenie	Sektor								
	2-0			2-1			2-2		
	Min	Max	Avg	Min	Max	Avg	Min	Max	Avg
Raspberry 1	-86	-49	-61	-78	-49	-62	-83	-53	-64
Raspberry 2	-83	-56	-69	-77	-55	-67	-81	-50	-65
Raspberry 3	-93	-45	-55	-77	-45	-58	-80	-45	-60
Raspberry 4	-84	-47	-59	-62	-38	-50	-80	-41	-56

Tabuľka 3 Maximálne, minimálne a priemerné hodnoty RSSI [dBm] prijímačov Arduino Nano IoT

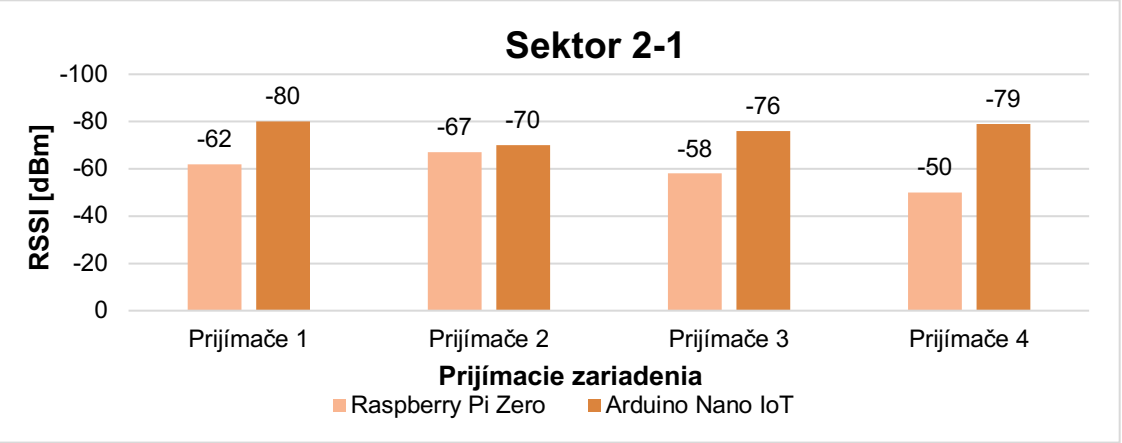
Prijímacie zariadenie	Sektor								
	2-0			2-1			2-2		
	Min	Max	Avg	Min	Max	Avg	Min	Max	Avg
Arduino 1	-92	-77	-84	-93	-75	-80	-87	-77	-81
Arduino 2	-82	-71	-76	-81	-65	-70	-87	-68	-78
Arduino 3	-86	-72	-77	-83	-72	-76	-86	-71	-76
Arduino 4	-83	-70	-76	-88	-71	-79	-82	-70	-75



Obrázok 2 Priemerné hodnoty [dBm] všetkých prijímacích zariadení v sektore 2-0

Na *Obrázku 2* sú znázornené priemerné hodnoty RSSI prijaté všetkými prijímacími zariadeniami nachádzajúcimi sa v každom bode v priestore v sektore 2-0. Priemerná hodnota RSSI prijímača Raspberry Pi Zero v bode 1 je **-61 dBm.** V bode 2 bola zaznamenaná priemerná hodnota RSSI **-69 dBm,** v bode 3 bola priemerná hodnota RSSI **-55 dBm** a v bode 4 bola **-59 dBm.**

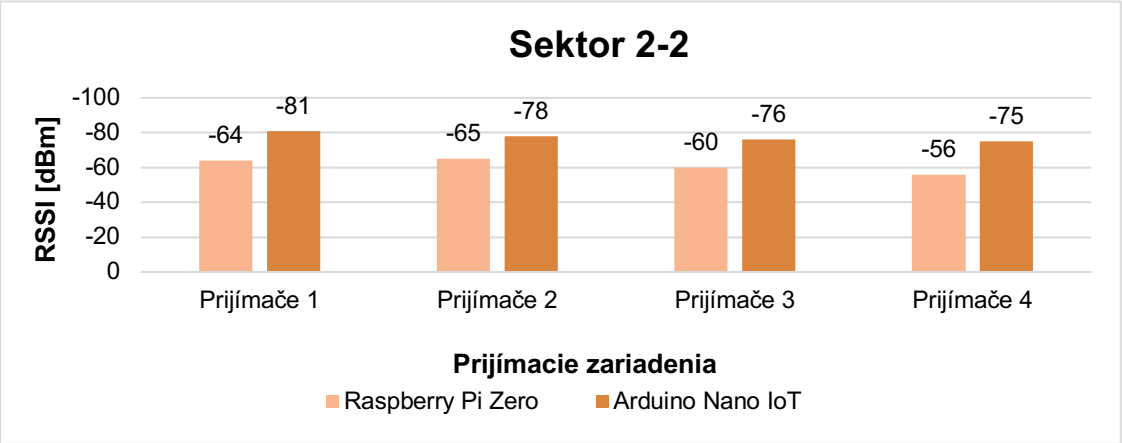
Získané výsledky ukazujú, že v sektore 2-0 dosahovali hodnoty RSSI nižšie hodnoty, keď ich prijímali prijímače Arduino Nano IoT. V bode 1 sa priemerná hodnota RSSI prijatá prijímačom Arduino Nano IoT znížila o **-23** dBm v porovnaní s prijímačom Raspberry Pi Zero. V bode 2 došlo k poklesu o **-7 dBm,** v bode 3 bola priemerná hodnota nižšia o **-22 dBm** a v bode 4 došlo k poklesu o **-17 dBm.**



Obrázok 3 Priemerné hodnoty [dBm] všetkých prijímacích zariadení v sektore 2-1

V sektore 2-1 bola priemerná hodnota RSSI prijímača Raspberry Pi Zero v bode 1 **-62 dBm.** V bode 2 bola priemerná hodnota **-67 dBm,** v bode 3 bola **-58 dBm** a v bode 4 bola priemerná hodnota **-50 dBm.**

Aj tu došlo k poklesu všetkých priemerných hodnôt prijímačov Arduino Nano IoT v porovnaní s prijímačmi Raspberry Pi Zero. Priemerná hodnota prijímača Arduino Nano IoT v bode 1 klesla o **-18 dBm,** v bode 2 došlo k poklesu o **-3 dBm,** v bode 4 klesla priemerná hodnota o **-18 dBm** a v bode 4 o **-29 dBm.**



Obrázok 4 Priemerné hodnoty [dBm] všetkých prijímacích zariadení v sektore 2-2

Keď bol beacon umiestnený v sektore 2-2, priemerná hodnota RSSI prijatá zariadením Raspberry Pi Zero v bode 1 bola **-64 dBm,** v bode 2 bola priemerná hodnota **-65 dBm,** v bode 3 bola priemerná hodnota **-60 dBm** a v bode 4 bola priemerná hodnota **-56 dBm.**

Rovnako ako v predchádzajúcich sektoroch boli priemerné hodnoty prijaté zariadením Arduino Nano IoT v sektore 2-2 nižšie ako hodnoty prijaté zariadením Raspberry Pi Zero. V bode 1 bola priemerná hodnota nižšia o **-17 dBm.** V bode 2 došlo k zníženiu priemernej hodnoty RSSI o **-13 dBm,** v bode 3 sa priemerná hodnota znížila o **-16 dBm** a v bode 4 o **-19 dBm.**

Spoľahlivosť prijímacích zariadení Raspberry Pi Zero a Arduino Nano IoT sa posudzovala na základe množstva hodnôt RSSI prijatých počas vykonaného testovania. Predpokladá sa, že čím väčší je počet prijatých hodnôt RSSI, tým presnejšia bude priemerná hodnota RSSI v danom sektore.

4 DISKUSIA A ZÁVER

Cieľom testovania bolo preskúmať spoľahlivosť 2 rôznych typov prijímacích zariadení na účely lokalizácie osôb a entít vo vnútri budov. Celkovo boli použité 4 zariadenia Raspberry Pi Zero a 4 zariadenia Arduino Nano IoT umiestnené na 4 miestach v priestore. Použitie viacerých prijímacích zariadení vyplynulo z potreby zabezpečiť maximálne pokrytie priestoru prijímacím signálom. V uzavretom priestore je potrebné použiť 2 alebo viac prijímacích zariadení, pretože použitie iba 1 prijímacieho zariadenia nepostačuje potrebám priestoru, ktorý má byť pokrytý prijímacím signálom. Dostatočné pokrytie

prijímacím signálom je potrebné na presné určenie polohy osôb a subjektov v uzavretom priestore.

Na základe vypočítaných priemerných hodnôt RSSI možno povedať, že v každom vybranom sektore prijímacie zariadenie Arduino Nano IoT zaznamenalo nižšie hodnoty RSSI v porovnaní s prijímacím zariadením Raspberry Pi Zero. Čím je hodnota RSSI vyššia, tým je signál kvalitnejší. Vykonali sa testy, pri ktorých sa ukázalo, že hodnotu RSSI ovplyvňuje vzdialenosť vysielacieho a prijímacieho zariadenia, výška inštalácie prijímacieho zariadenia a rôzne prekážky prítomné v priestore. V prípade porovnania prijímacích zariadení a ich vplyvu na hodnoty RSSI môže byť faktorom spôsobujúcim zníženie hodnôt RSSI prijímaných zariadením Arduino Nano IoT rozdielna prijímacia schopnosť rôznych prijímacích zariadení alebo výkonnosť zariadení.

Pri spracovaní získaných výsledkov testov sa zistilo, že väčší počet údajov odoslaných zo zariadenia Raspberry Pi Zero sa na server uložil v intervale 5 minút. Počet hodnôt RSSI prijatých zariadením Raspberry Pi Zero sa pohyboval od 1000 do 1200 údajov. Na základe stanovených podmienok sa však spracovalo 1000 údajov. Počet hodnôt RSSI prijatých zariadením Arduino Nano IoT bol výrazne nižší, v rozsahu 300 - 400 údajov. Tento jav nastal v dôsledku neschopnosti zariadenia Arduino Nano IoT súčasne prijímať vysielané signály z Beaconov a odosielať údaje na server. Zariadenie umožňuje prijímať signály vysielané Beaconmi v určitom časovom intervale. Potom odošle údaje na server, pričom v čase odosielania je zariadenie z hľadiska funkcie prijímania signálov neaktívne. Na základe tejto skutočnosti možno konštatovať, že prijímacie zariadenie Raspberry Pi Zero je spoľahlivejšie z hľadiska množstva prijatých údajov. V tom spočíva nevýhoda implementácie zariadenia Arduino Nano IoT. Problém sa dá vyriešiť použitím 2 zariadení Arduino Nano IoT, pričom jedno zariadenie by bolo prijímačom a druhé by fungovalo ako vysielač. Implementácia samostatných zariadení na prijímanie a odosielanie údajov však predstavuje vyššie finančné náklady. Rýchlosť odosielania údajov závisí aj od komunikácie v rámci internetovej siete, množstva a veľkosti odosielaných údajov.

Testovaním sa zistilo, že rôzne typy prijímacích zariadení môžu mať rôznu schopnosť prijímať signály. Schopnosť rôznych zariadení prijímať vysielané signály sa líši v závislosti od výkonu, kalibrácie systému, nainštalovaného softvéru alebo rôznych priestorových podmienok. Vzhľadom na typ systému, kvalitu snímania a jeho spoľahlivosť je vždy potrebné kalibrovať systém v konkrétnom priestore, pretože každý priestor sa líši v závislosti od typu poskytovaných služieb, usporiadania, stavebných prvkov, prítomných prístrojov alebo technického vybavenia. Tieto faktory sa musia zohľadniť, pretože môžu mať významný vplyv na presnosť určovania polohy v uzavretých priestoroch.

Vzhľadom na preukázané rozdiely medzi jednotlivými vysielacími zariadeniami je dôležité zohľadniť technické parametre a možnosti zariadení a

výber prispôsobiť požiadavkám kladeným na funkčnosť a ich implementáciu v konkrétnom priestore.

POĎAKOVANIE

Príspevok vznikol s podporou projektu „Kompetenčné centrum kybernetickej bezpečnosti UNIZA“, č. projektu 17R05-04-V01-00005, financovaného Európskou úniou - NextGenerationEU, v rámci Plánu obnovy a odolnosti Slovenska.

LITERATÚRA

[1] PHILIPS, D. R., SALAMI, E. et al. 2023. Location Accuracy Optimization in Bluetooth Low Energy (BLE) 5.1-Based Indoor Positioning System (IPS) - A Machine Learning Approach. In: *IEEE Access.* Roč. 11, s. 140186 – 140201.

[2] MIER, J., ALCÁZAR, A.J. et al. 2019. At a glance: Indoor Positioning Systems technologies and their applications areas. In: *ICITS*. s. 1-10.

[3] OBRETIN, A. M. 2020. Infrastructure free indoor positioning system. S. 124 – 133, DOI: 10.2478/picbe-2020-0013.

[4] MANEERAT, K., KAEMARUNGSI, K. 2020. Performance Improvement Design of Bluetooth Low Energy-Based Wireless Indoor Positioning Systems. In: *Mobile Information Systems*. DOI: 10.1155/2020/8891856

[5] JAILANI, N.S.S. et al. 2022. Indoor Positioning System: A review. In: *IJACSA*. Roč. 13, s. 477–490.

[6] SAID, A. et al. 2021. Implementing Associated Routing Protocol for Bluetooth Low Energy Devices. In: *IOSR-JCE*. Roč. 23, č. 6, s. 26-32.

[7] ČABARKAPA, D. et al. 2015. Comparative analysis of the Bluetooth Low-Energy indoor positioning systems. In: *TELKSIS.*

[8] YANG, J. et al. 2019. Beyond Beaconing: Emerging Applications and Challenges of BLE. In: *Ad Hoc Networks Journal*. Roč. 97, s. 1-18.

[9] POSDORFER, W., MAALEJ, W. 2016. Towards Context-aware Surveys Using Bluetooth Beacons. In: *Procedia Computer Science.* Roč. 83, s. 42-49.

[10] NONALINSAVATH, K. et al. 2020. Integration of Indoor Localization System using Wi-Fi Fingerprint, Bluetooth Low Energy Beacon and Pedometer Based on Android Application Platform. In: *International Journal of Intelligent Engineering and Systems*. Roč. 13, č. 4, s. 171-181.

[11] ZHANG, X., ZHANG, S. 2022. Regional Double-Layer, High-Precision Indoor Positioning System Based on iBeacon Network. In: *Mathematical Problems in Engineering.* DOI: 10.1155/2022/8673083.

[12] XU, G. 2021. Method of Enhancing the Accuracy of Indoor Positioning (RSSI to UL-AOA). In: *Journal of Physics: Conference Series.* 1871(1):012076. DOI: 10.1088/1742-6596/1871/1/012076.

„POST-MARKET CLINICAL FOLLOW-UP“ AKO NÁSTROJ BEZPEČNOSTI V ZDRAVOTNÍCTVE

Andrej Smetánka[1], Jan Rybář[2], Jana Gerneschová[3]

ABSTRAKT

Konferenčný príspevok sa zaoberá významom a aplikáciou klinických sledovaní po uvedení zdravotníckych zariadení a technológií na trh. PMCF predstavuje kontinuálny proces, ktorým sa monitorujú a vyhodnocujú dlhodobé účinky
a bezpečnosť produktov, ktoré už boli uvedené na trh a sú v klinickom použití. V príspevku sa analyzujú metódy zberu a vyhodnocovania dát, ako aj regulácie, ktoré zabezpečujú dodržiavanie požiadaviek na klinické sledovanie produktov. Dôležitým aspektom je aj zapojenie zdravotníckych profesionálov a pacientov do sledovania a reportovania nežiaducej reakcie. Príspevok sa venuje aj výzvam, ktoré PMCF prináša, ako napríklad integrácia medicínskej metrológie, zabezpečenie kvality dát, efektívnosť monitorovania a zlepšovanie komunikácie medzi výrobcami, regulačnými orgánmi a zdravotníckymi zariadeniami.

Kľúčové slová
PMCF, zdravotníctvo, bezpečnosť, medicínska metrológia

ABSTRACT

The conference paper deals with the importance and application of post-marketing clinical follow-up of medical devices and technologies. PMCF is a continuous process that monitors and evaluates the long-term effects and safety of products that have already been launched on the market and are in clinical use. The paper analyzes the methods of data collection and evaluation, as well as the regulations that ensure compliance with the requirements for clinical follow-up of products. An important aspect is also the involvement of healthcare professionals and patients in the monitoring and

1 Ing. Andrej Smetánka, Strojnícka fakulta, Slovenská technická univerzita v Bratislave, Nám. slobody 17, 812 31, Bratislava, +421 918 258 757, andrej.smetanka@stuba.sk
2 doc. Mgr. Ing. Jan Rybář, PhD., Strojnícka fakulta, Slovenská technická univerzita v Bratislave, Nám. slobody 17, 812 31, Bratislava, +421 949 611 537, jan.rybar@stuba.sk
3 Ing. Jana Gerneschová, Strojnícka fakulta, Slovenská technická univerzita v Bratislave, Nám. Slobody 17, 812 31, Bratislava; Český metrologický institut, Laboratoře primární metrologie Praha, V Botanice 1504/4, 150 72, Praha - Smíchov, +420 725 839 912, jana.gerneschova@cmi.gov.cz

reporting of adverse reactions. The paper also addresses the challenges that PMCF brings, such as the integration of medical metrology, ensuring data quality, monitoring efficiency and improving communication between manufacturers, regulatory authorities and healthcare facilities.

Key words
PMCF, healthcare, safety, medical metrology

1 ÚVOD DO RIEŠENEJ PROBLEMATIKY

Jedným zo základných pilierov moderného zdravotníctva je bezpečnosť pacientov. Každá zdravotnícka pomôcka alebo zariadenie, ktoré je uvedené na trh, môže mať potenciálny vplyv na zdravie pacienta. Preto je nevyhnutné zabezpečiť, aby tieto produkty nepredstavovali riziko pre používateľov (ani lekárov) a aby ich dlhodobá účinnosť bola v súlade s očakávaniami.

V tejto súvislosti zohráva kľúčovú úlohu monitorovanie produktov aj po ich uvedení na trh. Pomocou kontinuálneho sledovania môžeme odhaliť možné zriedkavé alebo oneskorené vedľajšie účinky, ktoré sa počas predchádzajúcich klinických skúšaní nemuseli prejaviť. Monitorovanie je základom dohľadu po uvedení na trh, ktorý umožňuje výrobcovi a regulačným orgánom identifikovať potenciálne riziká a včas prijať nápravné opatrenia.

Post Market Clinical Follow-up (PMCF) predstavuje systematický proces sledovania zdravotníckych pomôcok, ktorého cieľom je ich dlhodobé monitorovanie a vyhodnocovanie bezpečnosti v reálnych podmienkach klinického používania. PMCF je systém klinického hodnotenia zdravotníckych pomôcok a ich kontinuálneho monitorovania po uvedení na trh [1,2].

2 NARIADENIE MDR V ZDRAVOTNÍCTVE

Post Market Clinical Follow-up vychádza z nariadenia Medical Device Regulatation (MDR) vydaného Európskym parlamentom a Radou EÚ (nariadenie 2017/745). MDR nahrádza predchádzajúce smernice 90/385 ES a 93/42 EHS, účinnosť nadobudla v máji 2021. Tento právny predpis prináša prísnejšie požiadavky na klinické hodnotenie, bezpečnosť a sledovanie zdravotníckych pomôcok po ich uvedení na trh a to s cieľom zvýšiť ochranu a pacientov a používateľov. MDR sa zameriava na zabezpečenie kvalitného dohľadu po uvedení na trh, pričom je dôraz kladený na kontinuálne monitorovanie a vyhodnocovanie bezpečnosti zdravotníckych pomôcok [1,2].

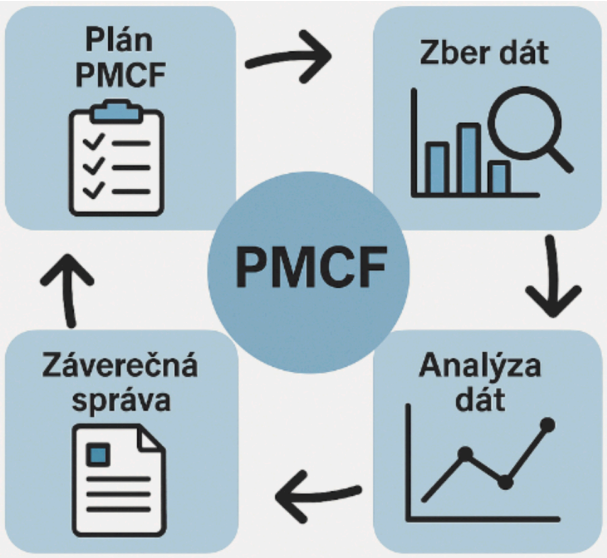
Hlavným cieľom MDR je posilniť bezpečnostné opatrenia týkajúce sa zdravotníckych pomôcok, zaviesť prísnejšie klinické hodnotenia a zabezpečiť lepší dohľad nad ich bezpečnosťou a výkonnosťou v reálnych podmienkach používania. Aby sa tieto ciele dosiahli, nariadenie zaväzuje výrobcov implementovať PMCF ako povinnú súčasť post-marketingového dohľadu [5].

Zavedenie MDR prinieslo niekoľko významných zmien v legislatíve:

- Zjednotenie legislatívy – nariadenie MDR harmonizuje pravidlá pre všetky členské štáty EÚ, čo predstavuje jednotný prístup k hodnoteniu a dohľadu nad zdravotníckymi pomôckami.
- Rozšírenie o ďalšie pojmy – zavádza nové kategórie zdravotníckych pomôcok.
- Rozšírenie databázy EUDAMED - EUDAMED, ako centralizovaný systém pre sledovanie zdravotníckych pomôcok, bol významne rozšírený a obsahuje viac údajov o zdravotníckych pomôckach, ich výrobcoch a klinických skúškach.
- Sprísnenie požiadaviek po uvedení na trh - MDR zavádza prísnejšie pravidlá pre dohľad a zodpovednosť výrobcov za monitorovanie dlhodobej bezpečnosti produktov [1, 5].

Podľa MDR je PMCF jeho neoddeliteľnou súčasťou a môžeme ho rozdeliť do viacerých krokov (obr.1) , ktoré zaisťujú systematický a efektívny proces monitorovania produktov:

1. Plánovanie - Tento krok zahŕňa stanovenie cieľov PMCF, vypracovanie plánu sledovania a identifikovanie potrebných dátových zdrojov. Je nevyhnutné definovať metódy zberu dát a časové rámce na ich analýzu.
2. Implementácia - V tejto fáze sa vykonáva samotné zahájenie klinických štúdií, sledovanie prieskumov medzi používateľmi alebo registrácií pacientov, ktorí používajú produkt.
3. Zber dát - dôkladné zhromažďovanie relevantných klinických údajov, ktoré sa vzťahujú na bezpečnosť, výkonnosť a akékoľvek nežiaduce účinky produktov. Tento krok môže zahŕňať prieskumy, klinické štúdie, analýzy zdravotných záznamov a spätnej väzby od zdravotníckych pracovníkov a pacientov.
4. Analýza dát - Po získaní dát nasleduje ich vyhodnotenie. Tento proces sa zameriava na identifikovanie potenciálnych problémov alebo rizík, ktoré sa môžu objaviť pri dlhodobom používaní zdravotníckych pomôcok. Výsledky tejto analýzy slúžia na identifikáciu prípadných nedostatkov alebo zlepšení produktov.
5. Záverečná správa - Po ukončení procesu monitorovania sa vypracuje správa, ktorá sumarizuje získané údaje, závery o bezpečnosti a výkonnosti produktu a odporúčania pre ďalšie kroky. Táto správa je súčasťou dokumentácie, ktorá je predkladaná regulačným orgánom, ako aj ostatným zainteresovaným stranám [4].



Obrázok 1 Kroky PMCF. [vlastné spracovanie]

EUDAMED (European Database on Medical Devices) je databáza spravovaná Európskou komisiou, ktorá slúži na centralizovanie a výmenu informácií o zdravotníckych pomôckach v Európskej únii. Tento systém poskytuje dôležité údaje o zdravotníckych produktoch, ich výrobcov a výsledkoch klinických štúdií a monitorovania.
S implementáciou MDR došlo k rozšíreniu a vylepšeniu EUDAMED, ktorá teraz zahŕňa širší okruh údajov, ktoré sa týkajú informácii o produktoch, výrobcoch, klinických údajov a hlásení o nežiadúcich účinkoch [3].

EUDAMED pozostáva zo šiestich hlavných modulov:

1. Registrácia subjektov – obsahuje informácie o výrobcoch, splnomocnených zástupcoch, dovozcoch a notifikovaných osobách.
2. Registrácia zdravotníckych pomôcok – obsahuje zoznam zdravotníckych pomôcok, ich triedenie, čísla UDI a certifikáty.
3. Notifikované osoby a ich certifikáty – poskytuje informácie o certifikátoch vydaných pre zdravotnícke pomôcky a o orgánoch zodpovedných za ich hodnotenie.
4. Klinické hodnotenie a dohľad po uvedení na trh (PMCF) –slúži na zhromažďovanie a správu dát o klinických sledovaniach, PMCF správach a výsledkoch dohľadu po uvedení na trh.
5. Dohľad nad trhom a vigilancia – obsahuje hlásenia o incidentoch, bezpečnostných oznámeniach (FSN - Field Safety Notices) a preventívnych opatreniach prijatých na ochranu zdravia.
6. Trh a dohľad nad distribúciou zdravotníckych pomôcok – sleduje tok zdravotníckych pomôcok na trhu a zabezpečuje, že sa dodržiavajú predpisy a tým aj bezpečnosť pacientov [3, 6].

Databáza EUDAMED sa podľa úrovni prístupu rozdelená na databázu EUDAMED s obmedzeným prístupom a verejne prístupnú databázu

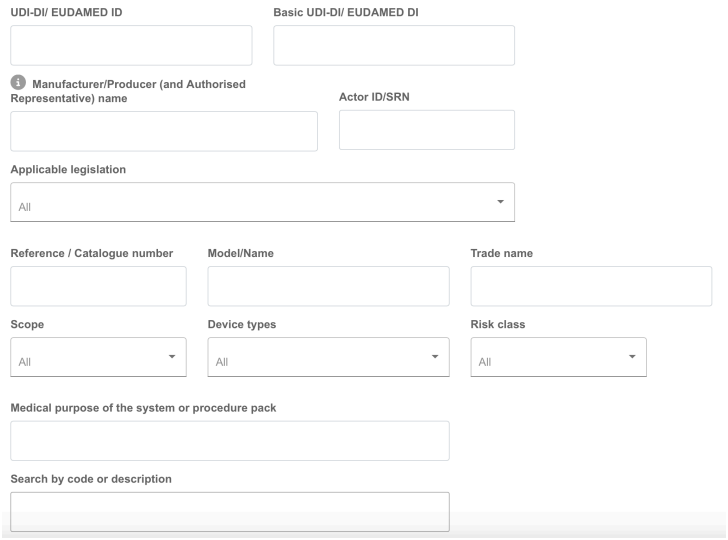
EUDAMED. Líšia sa okrem dostupnosti aj v úrovni detailov a rozsahu dostupných informácii [3, 6].

Verejne prístupná databáza

Poskytuje prístup k obmedzeným informáciám, ktoré sú relevantné hlavne pre širokú verejnosť, zdravotníckych profesionálov a výskumníkov. Medzi verejne dostupné dáta patria:

- Informácia o výrobcovi – jeho ID, krajinu pôvodu, kontaktné údaje
- Základné UDI informácie – UDI identifikačné čísla, kompletný názov, špecifikácia prostriedku
- Certifikáty
- Detailné UDI-DI informácie – status (na trhu/stiahnutý z trhu), doplňujúce informácie o prostriedku (podmienky použitia, a iné)
- Distribuované krajiny

Verejná databáza však neobsahuje podrobnosti o hlásených nežiaducich účinkoch alebo správach PMCF [6,7].



Obrázok 2 EUDAMED formulár. [6]

Databáza s obmedzeným prístupom

Je neverejná a teda prístupná iba autorizovaným používateľom, ako sú:

- Regulačné orgány (napr. Európska komisia, štátne dozorné orgány)
- Notifikované osoby hodnotiace zdravotnícke pomôcky
- Výrobcovia zdravotníckych pomôcok a ich splnomocnení zástupcovia

Neverejná databáza obsahuje:

- Podrobné informácie o PMCF správach a ich výsledkoch
- Hlásenia o nežiaducich udalostiach a opatreniach na minimalizáciu rizika
- Interné regulačné hodnotenia a rozhodnutia týkajúce sa bezpečnosti zdravotníckych pomôcok

Z dôvodu ochrany citlivých dát a obchodných tajomstiev nie sú tieto informácie dostupné verejnosti [6,7].

3 PRÍKLAD PRIAMEJ APLIKÁCIE PMCF

Výrobca zdravotníckych pomôcok uvádza na trh nový typ digitálneho tlakomeru. Tento tlakomer je vybavený automatickým meraním krvného tlaku a pulzu. Pred uvedením na trh prešiel všetkými klinickými skúškami a získal certifikáciu podľa MDR. Keďže ide o zdravotnícku pomôcku určenú na pravidelné meranie krvného tlaku u pacientov, výrobca je povinný vykonávať PMCF na monitorovanie jeho bezpečnosti a účinnosti v reálnych podmienkach používania.

Tabuľka 6 Technická špecifikácia - krvný tlakomer Omron RS7 Intelli IT. [5]

Rozsah merania	Tlak manžety	(0 až 299) mm Hg
	Systolický tlak	(60 až 260) mm Hg
	Diastolický tlak	(40 až 215) mm Hg
	Tepová frekvencia	(40 až 180) Bpm
Okolité podmienky	Teplota vzduchu	(5 až 40) °C
	Tlak vzduchu	(80 až 105) kPa
Dovolená chyba	Tlak	(± 3) mm Hg
Metóda merania		Oscilometrická, automatické nafukovanie a meranie

Kroky PMCF v modelovej situácii:

1. **Plánovanie PMCF**
   - Monitorovanie dlhodobej bezpečnosti tlakomeru a presnosti merania.
   - Identifikácia možných technických nedostatkov, ako je nepresnosť merania alebo porucha prístroja.

2. **Implementácia PMCF**
    - Zavedenie systému na hlásenie incidentov, kde môžu pacienti a lekári nahlásiť technické alebo zdravotné problémy spojené s používaním tlakomeru.
    - Pravidelné dotazníky pre pacientov a lekárov hodnotiace presnosť merania, jednoduchosť použitia a spoľahlivosť prístroja.

3. **Zber dát**
    - Lekári a zdravotnícke zariadenia pravidelne odosielajú hlásenia o nepresnostiach meraní alebo sťažnostiach pacientov.
    - Výrobca analyzuje údaje zo servisných centier, kde sa tlakomer opravuje alebo vymieňa kvôli poruchám.
    - Údaje sa zhromažďujú v centrálnej databáze a porovnávajú sa s informáciami z verejnej a neverejnej časti EUDAMED.

4. **Analýza dát**
    - Po určitej dobe sa ukáže, že u 4 % používateľov tlakomer vykazuje nepresnosti merania pri nízkych teplotách.
    - Výrobca identifikuje, že problém súvisí s kalibráciou snímačov, ktoré sú citlivé na teplotné výkyvy.
    - Výsledky sa porovnajú s údajmi z EUDAMED, kde sa nachádzajú podobné prípady hlásené inými výrobcami.

5. **Záverečná správa a opatrenia**
    - Výrobca pripraví podrobnú správu o zisteniach a navrhne preventívne opatrenia – úpravu výrobného procesu na zvýšenie odolnosti voči teplotným zmenám.
    - Správa sa predloží regulačným orgánom a zdravotníckym zariadeniam používajúcim tlakomer.
    - Výrobca vykoná úpravy v konštrukcii zariadenia a aktualizuje návod na použitie, kde odporúča správne skladovanie a používanie pri stabilných teplotách [6,7].

Modelová situácia pre krvný tlakomer ukazuje, ako PMCF pomáha identifikovať a riešiť problémy v reálnom používaní zdravotníckych pomôcok. Systematický prístup k monitorovaniu a analýze údajov zabezpečuje, že tlakomer zostáva nielen funkčný ale predovšetkým bezpečný pre pacientov. Bez priebežného monitorovania by problém mohol ostať neodhalený a viesť k vážnym zdravotným rizikám pre pacientov. Integrácia PMCF v rámci MDR zabezpečuje, že zdravotnícke pomôcky na trhu sú nielen plne funkčné, ale aj bezpečné pre dlhodobé klinické použitie.

Tabuľka 7 Vybrané parametre z databáty EUDAMED. [8]

Výrobca	OMRON Healthcare Co., Ltd.
ID výrobcu	JP-MF-000007213
Platný legislatívny predpis	MDR 2017/745
UDI-DI	4015672111174T
Trieda rizika	IIa
Označenie	Z1203020302: Neinvazívny krvný tlakomer
Status	Na trhu v EÚ
Členská krajina v ktorej vstúpil na trh	Holandsko

DISKUSIA A ZÁVER

PMCF zohráva kľúčovú úlohu v oblasti bezpečnosti zdravotníckych pomôcok a produktov po ich uvedení na trh. Tento proces zahŕňa systematické sledovanie a hodnotenie zdravotníckych produktov v reálnych podmienkach, kde sa odhaľujú riziká, ktoré nemusia byť identifikované počas klinických skúšok pred uvedením na trh. V súčasnosti sa zvyšuje tlak na zabezpečenie nielen kvality, ale aj bezpečnosti výrobkov, ktoré sú uvedené na trh. S rastúcim počtom zdravotníckych pomôcok a technológií, ako aj s ich čoraz zložitejšími mechanizmami, sa stáva PMCF nevyhnutným nástrojom na identifikáciu dlhodobých alebo zriedkavých nežiaducich účinkov, ktoré sa môžu objaviť až po uvedení produktu do širokého klinického prostredia [7].
Efektívny PMCF si vyžaduje spoluprácu medzi výrobcom, regulátorom a poskytovateľmi zdravotnej starostlivosti, aby sa zabezpečila maximálna ochrana zdravia verejnosti. Tento proces zaručuje, že zdravotnícke pomôcky a technológie na trhu budú aj naďalej spĺňať požiadavky na bezpečnosť a kvalitu, čím sa minimalizuje riziko nežiaducich účinkov a zvyšuje dôvera v zdravotnícke systémy. K uvedenému prispieva aj databáza EUDAMED a komplexne nariadenie MDR.

POĎAKOVANIE

Autori tohto príspevku ďakujú Strojníckej fakulte Slovenskej technickej univerzity v Bratislave, Českému metrologickému inštitútu, grantovej agentúre KEGA projektu číslo 024STU-4/2023 (Budovanie laboratória medicínskej metrológie), grantovej agentúre APVV projektu číslo APVV-21-0216 (Pokročilé matematické a štatistické metódy pre meranie a metrológiu) a grantovej agentúre APVV projektu číslo APVV-21-0195 (Výskum možnosti digitálnej transformácie kontinuálnych dopravných systémov) za ich podporu.

LITERATÚRA

[1] MOHN, D.; ZEHNDER, M.; *The medical device regulation (MDR) from a dental perspective.* Frontiers in Dental Medicine [online]. 23. marec 2023, roč. 4, článok 1155820[cit.2025-04-02]. Dostupné na: https://www.zora.uzh.ch/id/eprint/253237/1/ZORA_pdf.pdf

[2] BIANCHINI, B.; FRANCESCONI, M.; TESTA, M.; TANASE, M.; GEMIGNANI, V.; Unique device identification and traceability for medical software: A major challenge for manufacturers in an ever-evolving marketplace, In: *Journal of Biomedical Informatics*, Roč. 93, 2019, Dostupné na:(https://www.sciencedirect.com/science/article/pii/S1532046419300681)
[3] *EUDAMED*. Scilife © Scilife N.V. [online]. [cit. 2025-04-02]. Dostupné na: https://www.scilife.io/glossary/eudamed
[4] *MDR a klinické dáta*. [online] [cit. 2025-04-02]. Dostupné na: https://www.biostatistika.cz/index.php?pg=mdr

[5] SMETÁNKA, A. *Implementácia systémov manažérstva kvality v laboratóriu medicínskej metrológie*. [Diplomová práca]. Slovenská technická univerzita. Strojnícka fakulta. Ústav automatizácie, informatizácie a merania. Vedúci záverečnej práce: doc. Mgr. Ing. Jan Rybář, PhD. Bratislava: SjF STU BA, 2024. 83s.

[6] EURÓPSKA KOMISIA. *EUDAMED*. [online]. [cit. 2025-03-22]. Dostupné na: https://ec.europa.eu/tools/eudamed/#/screen/home

[7] EURÓPSKA KOMISIA. *Prehľad*. [online]. [cit. 2025-03-22]. Dostupné na: https://health.ec.europa.eu/medical-devices-eudamed/overview_sk?prefLang=sk

[8] *EUDAMED*. [online]. [cit. 2025-04-02]. Dostupné z: https://ec.europa.eu/tools/eudamed/#/screen/search-device/27dc9805-94d4-40d2-b9a2-eae66239a24e

EXPLOITING TRUST: HOW SOCIAL ENGINEERING THRIVES AND WHY ZERO TRUST MODEL MIGHT BE THE SOLUTION

Marek Švaňhal[1]

ABSTRAKT

V digitálním věku se důvěra stala výhodou i přítěží. Podporuje spolupráci a efektivitu, ale zároveň vytváří zranitelná místa, která sociální inženýři využívají prostřednictvím podvodů, manipulace a vydávání se za umělou inteligenci. Rostoucí sofistikovanost kybernetických hrozeb – poháněná technologií deepfake, behaviorálním profilováním a rozsáhlými phishingovými kampaněmi – donutila odborníky na kybernetickou bezpečnost přehodnotit tradiční bezpečnostní paradigmata. Příspěvek zkoumá model Zero Trust jako nezbytnou reakci na tyto vyvíjející se hrozby a zdůrazňuje jeho úlohu při zmírňování vektorů útoků zaměřených na člověka. Na rozdíl od tradičních bezpečnostních rámců, které předpokládají důvěru v sítích, model Zero Trust funguje na principu průběžného ověřování, což minimalizuje úspěšnost útoků sociálního inženýrství. Navzdory svým výhodám však není bez omezení – jeho implementace může vést k únavě z bezpečnosti, zvýšené provozní režii a odporu zaměstnanců, kteří jej vnímají jako omezující/zpomalující.

Klíčová slova:

Sociální inženýrství, kybernetická bezpečnost, phishing, Zero Trust, lidský faktor, důvěra.

ABSTRACT

In the digital age, trust has become both an asset and a liability. It promotes collaboration and efficiency, but it also creates vulnerabilities that social engineers exploit through deception, manipulation and impersonation. The increasing sophistication of cyber threats – driven by deepfake technology, behavioural profiling and large-scale phishing campaigns – has forced cybersecurity experts to rethink traditional security paradigms. This paper explores the Zero Trust model as a necessary response to these evolving threats and highlights its role in mitigating human-centric attack vectors. Unlike

1 Marek Švaňhal Ing., Univerzita Tomáše Bati ve Zlíně, m_svanhal@utb.cz

traditional security frameworks that assume trust in networks, the Zero Trust model operates on the principle of continuous authentication, which minimizes the success of social engineering attacks. However, despite its benefits, it is not without its limitations – its implementation can lead to security fatigue, increased operational overhead and employee resistance who perceive it as limiting/slowing them down.

Keywords:

Social engineering, cybersecurity, phishing, Zero Trust, human factor, trust.

1 INTRODUCTION

Trust has long been the foundation of human civilization. It enables cooperation, facilitates trade, and builds the relationships that hold societies together. Without trust, economies would stagnate, governments would fail, and technological advancements would struggle to gain adoption. However, while trust is essential for progress, it is also a significant vulnerability—one that has been exploited for centuries by those seeking to manipulate human behaviour. From con artists and scammers to modern cybercriminals, deception has always thrived by exploiting trust rather than breaking through technical barriers. Christopher Hadnagy [1] explains that trust is not just an emotion—it is a cognitive process shaped by predictability, familiarity, and perceived authority. Social engineers understand this dynamic and use it to their advantage, crafting attacks that mimic trusted sources, create urgency, and manipulate emotions. Unlike traditional cyberattacks, which rely on exploiting software vulnerabilities, social engineering bypasses technology altogether, targeting the human factor as the weakest link in security.

For example, phishing—a widespread and highly effective social engineering tactic—exploits trust in established communication channels. A well-crafted email that appears to be from a familiar source, such as a CEO or IT administrator, can trigger immediate compliance, especially when urgency is introduced. Veitaite [2] and Pimentel & Steinmetz [3] emphasize that social engineering attacks succeed not because of technological flaws, but because they manipulate human psychology—exploiting emotions like fear, curiosity, and urgency to override critical thinking. The success of these attacks demonstrates that even in organizations with robust security infrastructures, human trust remains the most easily exploited vulnerability.

As technology advances, so too do the methods used to manipulate trust. Deepfake technology, AI-generated phishing emails, and behavioural profiling have made deception more convincing and scalable than ever before. Attackers no longer need to rely on crude impersonations or poorly worded emails; instead, machine learning algorithms can generate messages, voices, and even video calls that are nearly indistinguishable from reality. This has led to a

growing crisis of trust in the digital world, where even well-informed individuals struggle to distinguish real from fake.

Dreeke [4] describes trust as a system built on predictability, transparency, and intent. However, in an era where AI-generated content can fabricate any of these elements, traditional notions of trust are being eroded. Organizations, governments, and individuals are being forced to rethink how trust is established, verified, and maintained in a world where deception can be automated at scale.

The Zero Trust model's foundations trace back to the 1990s. In April 1994, Stephen Paul Marsh, in his doctoral thesis "Formalising Trust as a Computational Concept" [5] at the University of Stirling, introduced the term "zero trust." Marsh examined trust as a measurable concept, arguing that it goes beyond fundamental human principles like integrity, fairness, legality, and personal evaluation. Building upon this academic groundwork, the Jericho Forum, established in the early 2000s, identified the limitations of traditional perimeter-based security models. In a 2004 keynote presentation at the Black Hat Briefings [6], Paul Simmonds, Global Information Security Director at ICI Plc. and a founding member of the Jericho Forum, discussed the concept of de-perimeterisation. He emphasized that the conventional perimeter security model was becoming obsolete due to evolving business practices and technological advancements. Simmonds highlighted the need for a new security model that focuses on protecting data rather than relying solely on perimeter defenses. This need has led to the rise of Zero Trust, a security model built on the principle of “never trust, always verify.” Unlike traditional security frameworks that assume trust within networks, Zero Trust operates under the assumption that every request, interaction, and identity must be continuously validated. It represents a paradigm shift in cybersecurity, replacing implicit trust with strict verification protocols.

As this paper will explore, Zero Trust is not merely a technical solution but a necessary adaptation to the evolving nature of deception. While it addresses many of the vulnerabilities associated with human trust, its implementation comes with its own challenges and limitations. Understanding both the strengths and drawbacks of Zero Trust is essential to navigating the complex landscape of trust, security, and social engineering in the modern digital world.

2 THE FRAGILE NATURE OF TRUST AND THE RISE OF ZERO TRUST SECURITY

Trust is one of the most fundamental aspects of human interaction. It dictates how we form relationships, collaborate, and build societies. Throughout history, trust was earned through direct experiences, reputations, and shared values. However, the digital transformation of human interaction has changed how trust is established, maintained, and—most critically—exploited.

This shift forces both individuals and organizations to adopt new verification mechanisms, as trusting our instincts alone is no longer sufficient. Robin Dreeke, in *The Code of Trust* [4], highlights that trust is not just an emotion but rather a process built on predictability, transparency, and shared intent. Traditionally, trust was reinforced through face-to-face interactions, long-term relationships, and verifiable reputations. However, in today's digital-first world, where interactions are often remote, instant, and anonymized, trust can be fabricated and exploited more easily than ever. Social engineers understand and manipulate these very elements, using AI to craft hyper-personalized deception that preys on human psychology and cognitive biases.

As these attacks grow in sophistication, the old adage of "trust but verify" has become obsolete—because even the verification process itself can be manipulated. Fraudsters no longer need to rely on gaining physical access or phishing for passwords when they can digitally forge identities, voices, and entire conversations in ways that are convincing even to trained professional, Hadnagy [1]. This escalation in deception tactics has led to a fundamental shift in cybersecurity, replacing implicit trust with a new paradigm: Zero Trust—where trust is no longer assumed but must be continuously verified and validated at every stage of an interaction.

3 ZERO TRUST AS A PSYCHOLOGICAL COUNTERMEASURE TO SOCIAL ENGINEERING

The Zero Trust model is often discussed in the context of network security, access controls, and authentication protocols, but its greatest impact lies in combating social engineering attacks. Social engineers exploit emotions—fear, urgency, trust, and authority—to deceive individuals into granting access, sharing credentials, or bypassing security measures. Zero Trust counteracts this by enforcing strict verification processes that reduce the effectiveness of deception-based attacks.

A key aspect of Zero Trust is continuous authentication, ensuring that even if an attacker gains access through manipulation, they must repeatedly verify their legitimacy. Potocký et al. [7] discuss how behavioural biometrics and real-time anomaly detection can help identify suspicious activity by analyzing typing speed, login patterns, and user behaviour. This disrupts the traditional tactics of social engineers, who rely on one-time deceptions to gain prolonged access.

Additionally, the least privilege principle ensures that even if an employee is compromised, attackers cannot escalate their access. Corbett and Nguyen [8] explain that microsegmentation and strict access controls prevent social engineers from moving laterally within an organization, limiting the damage they can cause. By removing broad access privileges, Zero Trust significantly

reduces the effectiveness of insider threats and credential-based attacks. However, despite its strengths, Zero Trust is not a silver bullet—and its implementation comes with significant challenges.

4 CHALLENGES AND LIMITATIONS OF IMPLEMENTING ZERO TRUST

While the concept of Zero Trust is powerful, its real-world application faces several obstacles—primarily stemming from human psychology, workplace culture, and operational complexity.

4.1 PSYCHOLOGICAL RESISTANCE: THE FATIGUE OF CONSTANT VERIFICATION

One of the biggest drawbacks of Zero Trust is that it contradicts the natural way humans build relationships and function in organizations. Employees who are accustomed to frictionless access may find Zero Trust restrictive, feeling like they are constantly being watched or second-guessed, Brower [9]. For instance, a long-time employee who suddenly needs multiple authentication steps to access a familiar system may interpret the process as a lack of trust from management rather than a security necessity. This perceived erosion of workplace trust can impact morale, collaboration, and efficiency.

Additionally, Zero Trust does not just affect employees—it also influences customers and external partners. If a business enforces strict verification policies, clients may experience frustration, viewing security measures as bureaucratic hurdles, rather than protective safeguards, Brower [9]. This creates a delicate balance between security and usability—one that organizations must navigate carefully.

Robin Dreeke [4] explains that people need to feel trusted to perform optimally. If security protocols become overly restrictive—requiring repeated authentication for even minor tasks—employees may experience “security fatigue” and seek shortcuts. Brumfield and Haugli [10] warn that when security measures become too cumbersome, users actively try to bypass them—leading to password sharing, unauthorized device usage, and even disabling security controls.

4.2 OPERATIONAL COMPLEXITY AND INCREASED COSTS

Zero Trust is not a plug-and-play solution; it requires constant monitoring, policy enforcement, and behavioural analysis. Hubbard and Seiersen [11] argue that while measuring cybersecurity risk is essential, many organizations lack the analytical tools to effectively quantify and assess risks in a Zero Trust environment.

In large organizations, the administrative overhead of continuously verifying thousands of employees, devices, and remote connections creates a significant burden on IT teams. Companies must invest in real-time monitoring tools, identity verification systems, and multi-factor authentication, which can be costly and complex to maintain.

For small and mid-sized businesses (SMBs), these financial and operational demands make full Zero Trust adoption impractical. As Corbett and Nguyen [8] highlight, many organizations underestimate the transition costs, leading to partial implementations that leave security gaps, ultimately undermining the effectiveness of Zero Trust principles.

4.3 CULTURAL SHIFTS: THE TENSION BETWEEN TRUST AND SECURITY

The biggest paradox of Zero Trust is that trust is necessary for collaboration, yet the model operates on distrust by default. While it improves security, it can also create a culture of suspicion where employees feel they are under constant surveillance.

Dreeke [4] emphasizes that trust is key to fostering innovation and teamwork. If employees perceive Zero Trust as an obstacle rather than a safeguard, it can lead to a disengaged workforce. This tension is particularly evident in hierarchical organizations, where senior executives may resist Zero Trust measures that limit their access or question their authority. Additionally, Zero Trust complicates internal workflows—delays in access approvals, excessive authentication requests, and frequent security checks can slow down productivity. If security becomes an inconvenience, employees may circumvent policies, inadvertently reintroducing vulnerabilities that attackers can exploit.

4.4 THE FALSE SENSE OF SECURITY: NO SYSTEM IS FOOLPROOF

Zero Trust significantly reduces attack opportunities, but it does not eliminate human error. Social engineering attacks are constantly evolving, and attackers are finding new ways to manipulate employees before verification even takes place.

For instance, deepfake phishing and AI-generated voice scams can bypass biometric authentication. If an employee believes they are receiving instructions from their CEO or IT administrator—especially if the communication mimics tone, speech, and urgency—they may still override security protocols under pressure.

Potocký et al. [7] highlight that no system can fully prevent psychological manipulation. Attackers exploit urgency, authority, and trust dynamics to pressure employees into taking action before security measures intervene.

4.5 BALANCING ZERO TRUST WITH HUMAN-CENTRIC SECURITY

Despite its challenges, Zero Trust remains one of the most effective defenses against social engineering threats [12]. However, for Zero Trust to truly work, it must be human-centric, ensuring that security does not come at the cost of trust, usability, or productivity.
Experts like Hubbard and Seiersen [11] suggest that organizations must:

- phase in Zero Trust gradually to minimize disruption,
- use behavioural analytics to reduce unnecessary authentication requests,
- prioritize usability so security measures don't feel like obstacles,
- train employees on why Zero Trust matters, ensuring they see it as protection rather than restriction.

Brumfield and Haugli [10] emphasize that Zero Trust should be adaptable, with policies evolving based on real-world behaviour and risk assessments. If implemented strategically, Zero Trust can enhance security without alienating employees or disrupting workflows.

CONCLUSIOION

Trust is both a strength and a vulnerability—it enables collaboration, yet it is easily exploited by attackers. Zero Trust is not about eliminating trust—it is about transforming it into something verifiable, adaptable, and resilient. In an era where deception is more sophisticated, scalable, and AI-driven than ever before, organizations must embrace a model that does not take trust for granted. However, for Zero Trust to succeed, it must not be a barrier to human productivity but rather a seamless, intuitive safeguard that protects people without alienating them. The future of cybersecurity does not lie in blindly rejecting trust; it lies in redefining it.

LITERATURA

[1] Hadnagy, Christopher. Social Engineering: The Science of Human

[2] Veitaite, Ilona, 2024. Challenges of Cyber Security in Modern Society: The Impact of Social Engineering. *Scientific and Practical Cyber Security Journal*. Roč. 2024, č. 8(4): 139. ISSN 2587-4667

[3] Pimentel, A., Steinmetz, K.F. Enacting Social Engineering: The Emotional Experience of Information Security Deception. *Crime Law Soc Change* 77, 341–361 (2022). https://doi.org/10.1007/s10611-021-09993-8

[4] Dreeke, R. (2017). *The Code of Trust: An American Counterintelligence Expert's Five Rules to Lead and Succeed*. St. Martin's Press
[5] MARSH, Stephen Paul, 1994. *Formalising trust as a computational concept*. Dissertation, vedoucí Thimbleby, Harold. University of Stirling: University of Stirling. http://hdl.handle.net/1893/2010.
[6] Simmonds, P. (2004) 'De-Perimetrisation This Decades Security Challenge'. Blackhat. https://www.blackhat.com/presentations/bh-usa-04/bh-us-04-simmonds.pdf
[7] S. Potocký, J. Štulrajter and M. Turčaník, "Advanced Industrial Espionage: Mobile Device as Anti-Forensic and Anonymization Tool," 2024 New Trends in Signal Processing (NTSP), Demanovska Dolina, Slovakia, 2024, pp. 1-8, doi: 10.23919/NTSP61680.2024.10726287.
[8] Corbett, C., Nguyen, C., Hongchai, D.M., Thorat, P., Prasad, P., von Schimmelmann, S., Weber, C.M., & Anderson, T.R. (2024). Power Resilience Planning under the Threat of Artificial Intelligence. *2024 Portland International Conference on Management of Engineering and Technology (PICMET)*.
[9] Brouwer WB, van Exel NJ, Koopmanschap MA, Rutten FF. Productivity costs before and after absence from work: as important as common? Health Policy. 2002 Aug;61(2):173-87. doi: 10.1016/s0168-8510(01)00233-0. PMID: 12088890.
[10] Brumfield, Cynthia a Haugli, Brian. Cybersecurity Risk Management. Wiley, 2021. ISBN 978-1-119-81630-0
[11] Hubbard, Douglas W. a Seiersen, Richard. How to Measure Anything in Cybersecurity Risk. Second Edition. Wiley, 2023. ISBN 978-1-119-89230-4.
[12] Aiello, Samuel T., "Prescriptive Zero Trust: Assessing the Impact of Zero Trust on Cyber Attack Prevention" (2024). *Masters Theses & Doctoral Dissertations*. 466. https://scholar.dsu.edu/theses/466

EXPERIMENTÁLNÍ URČENÍ OPTIMÁLNÍHO PODTLAKU PRO MĚŘENÍ VE VÝBUCHOVÉM AUTOKLÁVU VA–250L

Kateřina Symonová[1]

ABSTRAKT

Příspěvek se zabývá experimentálním stanovením počátečního pracovního podtlaku pro výbuchový autokláv VA–250L o objemu 250 litrů. Vzhledem k nestandardizované velikosti komory nelze přímým způsobem aplikovat normované vstupní parametry dle ČSN EN 14034. Cílem experimentů bylo určit optimální hodnoty podtlaku pro čtyři různé rozvířovací tlaky a analyzovat vliv zpoždění iniciace na míru homogenizace prachové atmosféry. Výsledky ukazují závislost potřebného podtlaku na zvoleném přetlaku a optimální interval iniciace mezi 450–550 ms. Provedené experimenty stanovují přesnější nastavení podmínek pro měření výbuchových charakteristik v zařízení mimo standardizované objemy.

Klíčová slova:
Výbuchový autokláv, optimalizace VA-250L, počáteční pracovní tlak, zpožděná iniciace.

ABSTRACT

This paper presents an experimental determination of the initial working vacuum for the VA–250L explosion chamber with an internal volume of 250 liters. Due to the non-standard chamber size, it is not possible to directly apply the standardized input parameters defined by ČSN EN 14034. The aim of the paper was to determine the optimal vacuum levels for four different dispersion pressures and to analyze the effect of ignition delay on the homogeneity of the dust-air mixture. The results show a clear dependence of the required vacuum on the selected overpressure and identify the optimal ignition delay range between 450–550 ms. The paper contributes to more accurate parameter settings for explosion testing in non-standard volume equipment.

Key words:
Explosion chamber, VA-250L optimalization, initial working pressure, delayed ignition.

1 Ing. Kateřina Symonová, Lumírova 630/13, 703 00, Ostrava-Výškovice, +420596992835, katerina.symmonova@vsb.cz

1 ÚVOD

Výbuchové autoklávy jsou často využívaným zařízením při experimentálním stanovování výbuchových charakteristik hořlavých látek a směsí. Tato zařízení se liší nejen konstrukcí, ale především objemem výbuchové komory, který zásadně ovlivňuje výsledné hodnoty měřených parametrů – zejména maximální výbuchový tlak, rychlost nárůstu výbuchového tlaku a z něj odvozenou kubickou konstantu. Využití různých objemů tak přináší v jednom směru jistou variabilitu výsledků.

Cílem tohoto příspěvku je experimentální stanovení optimální hodnoty počátečního podtlaku v komoře nestandardizovaného výbuchového autoklávu o objemu 250 litrů. Tento výbuchový autokláv díky své specifičnosti neumožňuje přímé přejímání výchozích parametrů z normovaných metodik určených například pro výbuchový autokláv o objemu 20 litrů. Vstupní data proto vychází z ČSN EN 14034 a prostřednictvím série experimentů jsou stanovovány specifické pracovní podmínky pro měření výbuchových charakteristik prachových směsí právě v tomto zařízení.

2 METODOLOGIE

Problematika výchozího optimálního nastavení výbuchového autoklávu se zakládá na hodnotách pracovních tlaků a hmotnostních koncentrací, které jsou definovány normovaným postupem dle ČSN EN 14034 *Stanovení výbuchových charakteristik rozvířeného prachu* [1]. Podle těchto vstupních hodnot byly experimentálně stanovovány rozdíly tlaků v jednotlivých fázích pracovního procesu.

Pro analýzu stavu prachových částic v závislosti na době zpoždění iniciace vycházel pracovní postup z experimentálního měření dle [2].

3 MĚŘENÍ VÝBUCHOVÝCH CHARAKTERISTIK

Signifikantním projevem je výbuch sám o sobě, jeho velikost ale může být ovlivněna mnoha faktory. Stanovení krajních, a tedy těch nejpalčivějších projevů lze pro látku stanovit tzv. výbuchové charakteristiky.

Komplexní shrnutí se projevuje tvarem výbuchové křivky. Z té je stanoven maximální výbuchový tlak a rychlost nárůstu výbuchového tlaku, přepočtem pak ještě kubické konstanta K_{st} nebo K_g. Tyto parametry definují měřítko výkonu výbušné směsi při její optimální koncentraci [3].

Výbuchové charakteristiky, stejně jako další vlastnosti hořlavých či výbušných látek a směsí (např. minimální iniciační energie) lze stanovit pomocí standardizovaných zařízení, jako jsou Hartmannova trubice nebo Godbert-Greenwaldova pec.

Právě pro stanovení maximálního výbuchového tlaku, rychlosti nárůstu výbuchového tlaku a kubické konstanty lze využít výbuchový autokláv. Často jsou využívány komory o vnitřním objemu 10, 20, 50 či 1000 litrů. S rostoucím objemem nádoby klesá rychlost nárůstu výbuchového tlaku a v této závislosti se mění i kubická konstanta.

3.1 OVLIVNĚNÍ VÝBUCHOVÝCH PARAMETRŮ

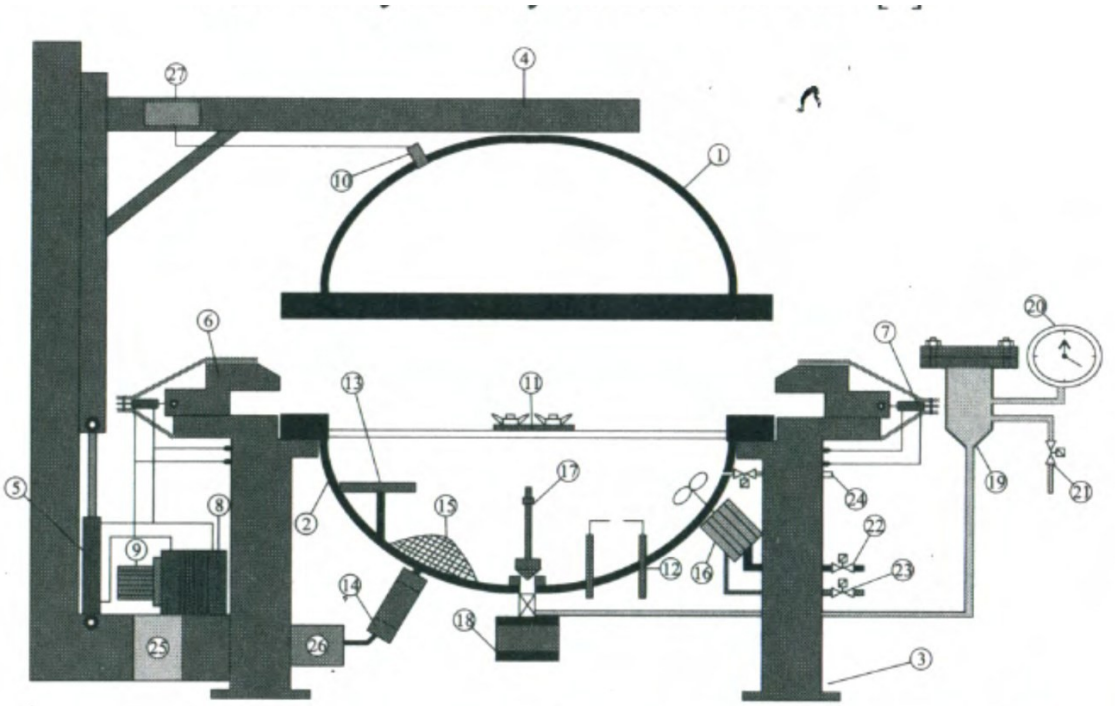
Výbuchové parametry testované látky či směsi se zákonitě mění s podmínkami uvnitř výbuchové komory, které jsou nastaveny v okamžik iniciace. Variacemi, které dokážou ovlivnit maximální výbuchový tlak, rychlost nárůstu výbuchového tlaku a kubickou konstantu lze chápat například počáteční teplotu výbušné atmosféry (která rozšíří meze výbušnosti), velikost či vlhkost rozvířovaných částic nebo míru homogenizace rozvířovaného látky.

V případě prachu se jedná o míru turbulentního proudění uvnitř komory a míru usazování již rozvířeného prachu. Právě homogenní směs je zcela zásadní pro rovnoměrný výbuch celého množství testované látky.

4 VA-250L

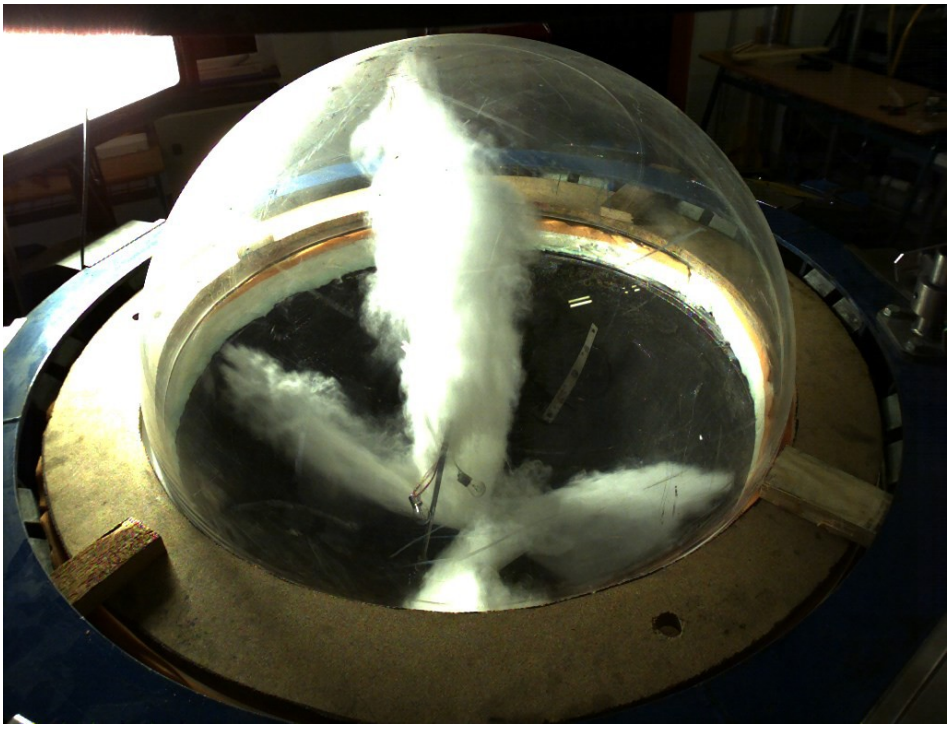
Výbuchový autokláv VA–250L je unikátním, ale nestandardizovaným zařízením pro měření výbuchových parametrů o objemu 250 litrů. Samotná komora autoklávu je složena ze dvou symetrických ocelových polokoulí a je umístěna ve střední části rámu. Spodní hemisféra je pevně připevněna k rámové konstrukci, zatímco horní hemisféra je připevněna k pohyblivému rámu, který slouží k otevírání a uzavírání výbuchové komory mezi jednotlivými experimenty. Ovládání komory probíhá díky jednočinnému hydraulickému válci, které ovšem dovoluje pouze dvě krajní polohy, a to *Otevřeno* a *Zavřeno.* V poloze *Zavřeno* jsou hemisféry blokovány proti oddálení hydraulicky ovládanými kameny. Prostor mezi polokoulemi je vyplněn pryžovým těsněním.

Z vnější části spodní polokoule jsou umístěna dvě čidla statického talku o rozsahu 4 a 16 barů, ventily pro nezávislý přívod dvou plynů, ventil pro odtlakování, výpusťový ventil a systém pomocných ovládacích prvků a eketroinstalace. Na horní polokouli je instalováno čidlo dynamického tlaku Saturn. Z boku je v konstrukci umístěn nerezový zásobník pro rozvířování, který je připojen k rozvířovacímu mechanismu skrz spodní polokouli. Na obrázku 1 je znázorněno blokové schéma celého autoklávu [2].



Obrázek 1 Blokové schéma výbuchového autoklávu VA-250L [2]

Rozvířovací mechanismus se skládá ze zásobníku, manometru, rozvířovacího nástavce a systému trubek a pneumatických ventilů. Rozvířovací nástavec zkosením stěn vnitřní části směřuje prach do pěti směrů, kdy čtyři z nich se rozbíhají v 90° rozmezí po stěnách spodní hemisféry a následně rotují po povrchu celé komory, pátý pak směřuje spodní části výbuchové komory kolmo vzhůru, viz obrázek 2 [2].



Obrázek 2 Mechanismus rozvířování částic prachu uvnitř komory

5 POSTUP MĚŘENÍ

Vzhledem ke specifičnosti výbuchového autoklávu nelze přejmout nastavení počátečních parametrů z normovaných postupů pro výbuchové komory o jiném objemu. Pro experimentální zkoušky výbušných prachů, plynů nebo hybridních směsí těchto fází lze ovlivnit parametry výbuchu několika cestami.

Aplikace prachu je vždy závislá na rozvířovacím systému, kde lze nastavit velikost používaného přetlaku. Po rozvíření se tlak v komoře zvýší a aby byl v momentu iniciace v komoře atmosférický tlak (101 325 Pa, respektive 1,013 bar) je potřeba před zahájením rozvířování komoru odtlakovat. Velikost podtlaku byla první částí experimentálních měření.

Výsledné výbuchové charakteristiky prachu či hybridní směsí mohou být ovlivněny mírou homogenizace látky v moment iniciace. Na zanalyzování stavu rozvířovaného prachu v závislosti na zpoždění iniciace se zaměřuje druhá sada experimentálních měření.

5.1 STANOVENÍ POČÁTEČNÍHO TLAKU V AUTOKLÁVU

Podle normy ČSN EN 14034 jsou definovány rozvířovací tlaky na 0,5–2 MPa s intervalem 0,5 MPa.[1] Tyto čtyři definované tlaky byly vstupní hodnotou pro jednotlivé série měření.

Pracovní postup spočíval v natlakování zásobníku a následném rozvíření. Pro potřebu těchto experimentů bude zachován pojem „rozvířování“ i přesto, že žádná látka rozvířována nebyla. Připojením dynamického čidla byl měřen absolutní talk uvnitř komory, a zároveň byl statickým čidlem měřen rozdíl tlaků. Zprůměrováním hodnot 10 opakování pro každý pracovní tlak byl nejdříve experimentálně stanoven přetlak po rozvíření při 0,5 MPa na 12,6 kPa (126 mbar), při 1 MPa na 23,1 kPa (231 mbar), při 1,5 MPa na 32,8 kPa (328 mbar) a při 2 MPa na 42,7 kPa (427 mbar).

Hodnotu podtlaku, vyžadovanou pro jednotlivé pracovní tlaky nelze stanovit pouze z matematického přepočtu. Snížení tlaku v komoře tak, aby v okamžiku iniciace odpovídaly podmínky atmosférickému tlaku tak byly stanoveny následující sadou experimentů. V komoře byl vytvořen podtlak nejdříve na základě matematického přepočtu vzniklého přetlaku a následně zahájen proces rozvířování. Po celou dobu byly monitorovány tlaky statickým i dynamickém čidlem. Výsledný podtlak, který je potřeba v komoře vytvořit je pro rozvířování při 0,5 MPa stanoven na 16,2 kPa (162 mbar), při 1 MPa na 28,1 kPa (281 mbar), při 1,5 MPa na 38,4 kPa (384 mbar) a při 2 MPa na 48,5 kPa (485 mbar).

5.2 DOBA ROZVIŘOVÁNÍ A ZPOŽDĚNÍ INICIACE

Rozvířovací proces je definovaným postupem podle ČSN EN 14034, na který ale úzce navazuje iniciace vzniklé výbušné atmosféry. Moment iniciace je zásadní chápat kvůli míře homogenizace testovaného vzorku. Zpožděná iniciace pak bude mít zásadní vliv na výbuchové charakteristiky testovaného látky vzhledem ke stavu rozvířovaného prachu.

Touto sadou experimentálních měření byl pozorován stav rozvířování, respektive míra usazování kukuřičného škrobu, rozvířovaného tlakem 20 bar (2 MPa).

Vrchní hemisféra výbuchového autoklávu byla nahrazena plexisklovou polokoulí o stejném vnitřním objemu, jako standardní hemisféra VA-250, díky čemuž bylo možné pozorovat a zaznamenat chování rozvířovaného prachu od zahájení rozvířovacího procesu až do momentu iniciace. Samotný iniciační zdroj byl simulován dvěma LED diodami (červené a zelené barvy). Moment rozsvícení diod znázorňuje zahájení iniciace.

Zpožděná iniciace byla pro tuto experimentální sadu stanovena v rozmezí 300-600 ms s intervalem 50 ms a porovnání stavu rozvířovaného prachu v čase je znázorněno na obrázku 3. Při iniciování výbušné atmosféry je prach stále v turbulentním stadiu, na snímcích lze jasně vidět proudy prachových částic, které nejsou rovnoměrně rozvířeny v definovaném objemu. S prodlužujícím se časem dochází k rovnoměrnému rozptýlení prachových částic a lze tak konstatovat, že ideální stav prachových částic je v rozmezí 450-550 ms po zahájení procesu rozvířování.

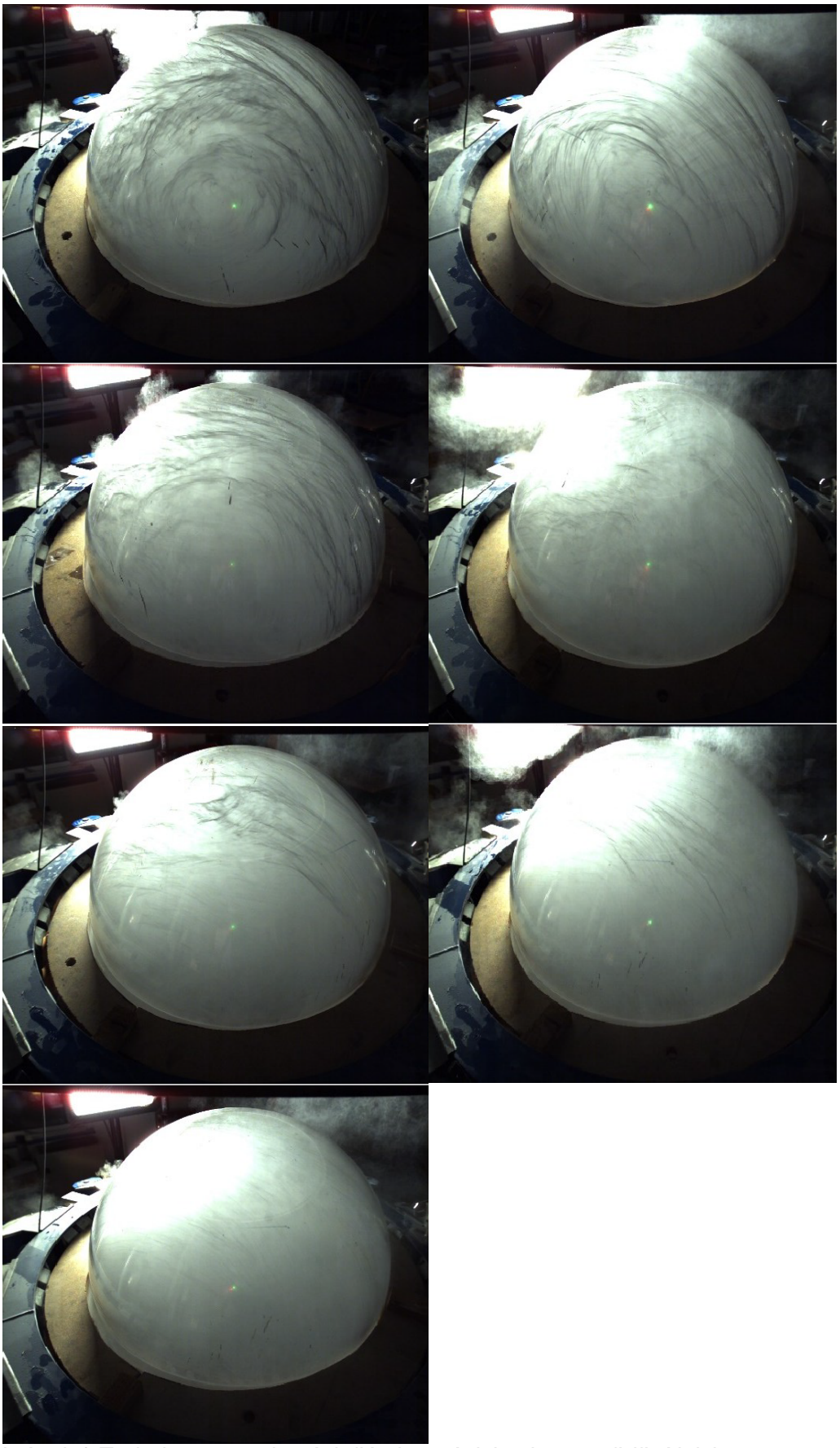
Na tyto vizuální výsledky bude navazovat sada experimentálních měření, kdy budou ověřovány výbuchové charakteristiky stejného vzorku.

300 ms / 350 ms

400 ms / 450 ms

500 ms / 550 ms

600 ms



Obrázek 3 Turbulence prachových částic v závislosti na zpoždění iniciace

6 ZÁVĚR

Pro experimentální měření ve výbuchovém autoklávu VA–250L byly stanoveny optimální hodnoty počátečního podtlaku, které umožní dosažení atmosférického tlaku v komoře v okamžiku iniciace rozvířené prachové směsi. Ze získaných dat lze stanovit konkrétní hodnoty potřebného poklesu pracovního tlaku, a to při rozvířovacím tlaku 0,5 MPa na 16,2 kPa, při 1 MPa na 28,1 kPa, při 1,5 MPa na 38,4 kPa a při 2 MPa na 48,5 kPa.

Ve druhé sadě experimentů byl pozprván dispergovaný stav prachových částic v čase. Tyto výsledky lze využít pro znalost homogenizace směsi a využití zpožděné iniciace. Rovnoměrného rozptýlení prachových částic je v tomto výbuchovém autoklávu dosaženo přibližně 450–550 ms po zahájení rozvířovacího procesu. Takto získané hodnoty jsou výchozími parametry pro další testování výbuchových charakteristik ve VA-250L a potvrzují nutnost individuální kalibrace zařízení mimo rámec standardních objemů.

LITERATURA

[1] [ÚNMZ] ÚAD PRO TECHNICKOU NORMALIZACI. ČSN EN 14034, Stanovení výbuchových charakteristik rozvířeného prachu. 2011.

[2] DAMEC, J. Protivýbuchová prevence I. Sdružení požárního a bezpečnostního inženýrství, 2005. ISBN 80-86111-21-0.

[3] LEPÍK, Petr, Jiří SERAFÍN a Miroslav MYNARZ. Ověření procesu rozvíření pšeničné mouky na výbuchovém autoklávu VA - 250. 2012.

OVERVIEW OF AUTONOMOUS TRAIN SYSTEMS AND THEIR SAFETY UP TO GRADE OF AUTOMATION (GOA) 4

Martin Václavík[1], Martin Haváček[2]

ABSTRACT

Railway transportation plays an important role in today's economy and green transformation. One of the big efforts is constant increasing of railway safety, efficiency and minimising operational costs. There is also a challenge of human resources in train operations. These issues are being solved in the development of autonomous train technology. However, a set of new challenges is presented. This paper examines the key challenges in safety of autonomous railway operation and presents methods to mitigate potential risks associated with autonomous railway operation such as obstacle detection or cybersecurity threats. The latter part of this study looks into the future perspectives of autonomous railway operations.

Key words:
Autonomous railway, grade of automation, railway safety, railway operation.

1 INTRODUCTION

Autonomous trains are an important part of current railway research. Their use in real-life operations can reduce operating costs and staff needs within the industry that is quite often subject to understaffing. The full deployment of this technology will also lead to increased efficiency, improved safety, better punctuality, and higher comfort for the passengers.

However to function properly, a very high safety standards need to be set, followed in the development and achieved in testing. There are many aspects to the safety of autonomous train operation. A train is a vehicle moving through an open environment, interacting with its surroundings. A big variety of obstacles might interfere with a movement of a train. To name a few, it might be a fallen tree, a car at a railway crossing, an unauthorised person in the railway line, or an animal crossing the tracks [1].

1 Ing. Martin Václavík, VŠB – Technická univerzita Ostrava, Fakulta strojní, 17. listopadu 2172/15, 708 00 Ostrava-Poruba

2 Ing. Bc. Martin Haváček, VŠB – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství, Lumírova 630/13, 700 30 Ostrava-Výškovice

Also, the railway system itself presents a complex set of rules, procedures and signalling methods and interlocking methods. This creates many layers that autonomous systems have to integrate and at which it needs to function properly to ensure a safety operation. To tackle this issue a complex architecture with various safety mechanisms and systems are being developed [2].

The first automated train in operation were introduced in 1968 on Victoria line in London Underground, however these were still overseen by a driver. The first fully automated railway system was opened in Kobe, Japan in 1981 named the Port Liner [3]. Today, we can already see more autonomous railway systems in operation. These however function on a separated infrastructure like subway or light rail systems, for example the DLR system in London, M4 underground line in Budapest or Copenhagen Metro lines M1 – M4.

This study evaluates current challenges in all grades of automation and discusses solutions ensuring that the highest safety standards are met. Attention is paid to technical, regulatory and operational measures.

2 SAFETY CHALLENGES IN AUTONOMOUS TRAIN OPERATIONS

There are 4 levels of automation of train driving, these are called grade of automation (GoA) named GoA 1 – GoA 4. Every level brings certain challenges and risks that need to be considered. According to UITP [4], these grades vary based on the automation level and level of human responsibility needed. We can theoretically also consider GoA 0, where the driver is fully responsible for all train driving operations. Under these circumstances, the biggest safety risk lies in the failure of human factor.

In GoA 1, the train is operated manually by the driver, however systems of automatic train protection are introduced. These can intervene in traction and brake systems to stop the train automatically, when needed. The biggest risk still lies within the mistake made by a human operator. A strong attention and adherence to the signals and potential obstacles is required from a driver. In an emergency, a driver is required to act cold-headed and handle the emergency.

GoA 2 relays on semiautomatic type of operation. The train can stop automatically at pre-defined stopping points (in some systems even at red signals), the driver is responsible for door operation, obstacle detection, handling of emergencies etc. The biggest risks associated with this type of operation is overreliance of a driver on automation system and attention loss. In case of any technical failure of automation system, a driver takes over controls and enters GoA 0 or GoA 1 operation (depending on the type and seriousness of failure).

In GoA 3, the driver is no longer in the cabin, the train handles stopping at pre-defined points and signals (if needed), however a train attendant is present on-board. An attendant operates train doors, handles emergency situations and gives departure acknowledgement signal to the system. As the presence of a driver is no longer required, the biggest risk lies in system failure. The system is also prone to any mistakes that might have been made in the development phase, e.g. while tackling a very non-standard and unlikely situation, that has not been tested. There is a big reliance on real-time monitoring and remote intervention of the system. As the operational entity is fully dependent on digital technologies, there is a serious threat of cyberattacks. In emergency situations, a train attendant is responsible for passenger management and their safety.

GoA 4 presents the highest grade of automation with unattended operation when the train is fully autonomous. The threats of autonomous system remain the same as in GoA 3, but there are also other risk factors, because a train is not attended anymore. In emergency a panic or chaos might burst among passengers, which can endanger them and slow down their evacuation.

The key elements of taking over the driver's role lies in perception, situation awareness, decision making, control tasks and communication. The recent technology of artificial intelligence and machine learning have greatly enabled the use and improvement of perception system technology and other parts of the system [5]. To understand more the operational concept, a simplified architecture is presented in *Figure 3*.

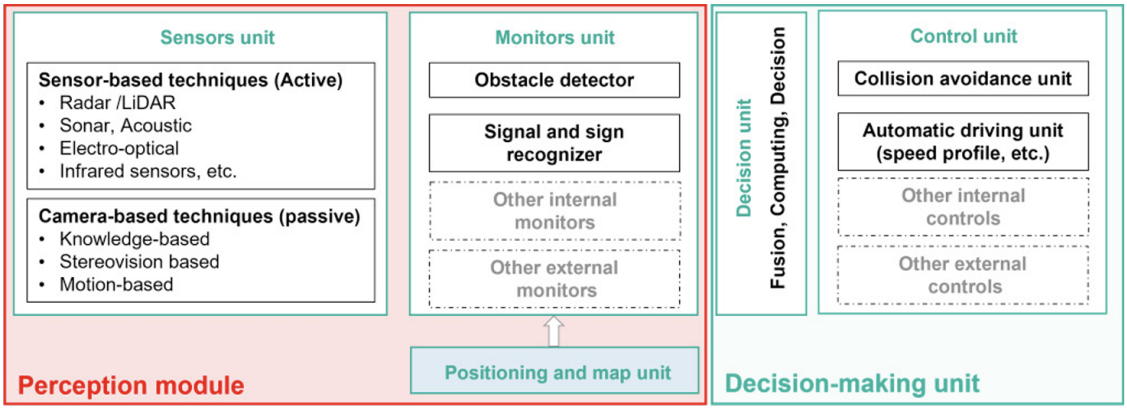


Figure 3: Simplified functional architecture of train autonomous driving system [5]

We can group the potential risks associated with an autonomous system into several categories:

- System Failures: any technical malfunction in the system or part of the system may influence its performance. As the system relays on sensorial units, camera units, monitoring units etc., failure of any of these systems can lead to operational risks and hazards [5].

- Obstacle Detection: autonomous trains rely only on sensorial input and its evaluation and decision made by decision unit. Many input data must be evaluated in real time. Unexpected obstacles and objects might appear on tracks, such as fallen tree, animals or trespassers, which if not detected and evaluated correctly within a very short time [6].
- Cybersecurity Threats: any unauthorised intervention with the system can disrupt railway operations or even posses a safety hazard [7].
- Emergency Response Limitations: in GoA 4 operation, with no staff onboard, any emergency situations must be resolved by the remote centre, response mechanisms and disciplined passengers [8].
- Interoperability Issues: a seamless implementation and integration of more levels of GoA must be considered and possible [9].

When considering a bigger picture, we must think about other trains on the infrastructure as well. Communication, interaction and awareness of other trains and entities sharing infrastructure (e.g. maintenance workers) is crucial for safety. There are measures coping with these issues, which include mainly usage of a traffic management system, radio controlled operation and communication and fail-safe train positioning.

3 SAFETY ASSURANCE STRATEGIES

To ensure a safe operation of autonomous trains, the beforementioned issues must be tackled. We can distinguish 3 categories of safety measures:

- Technical safety measures,
- Regulatory and standardization measures,
- Operational measures.

Technical safety measures are designed to mitigate risks connected with autonomous operations by using advanced technologies with redundancy. The redundancy ensures that in case of failure of one sub-system, the whole system does not fail. The systems are backed up and might use a dual channel design pattern. This architecture takes 2 independent inputs evaluated by 2 independent units, which must obtain the same result (in different ways). The probability of failure is the product of probabilities of both systems failure. These systems need to be certified for safety integrity level SIL-4, which is the highest integrity level. Another form of ensuring the highest safety standards is achieved by sensor fusion, which is mainly used in obstacle detection functionality. By utilizing AI algorithms and inputs from various sensors (LiDAR, radar, camera) a probability of correctly detecting the obstacle is further enhanced [8]. Predictive maintenance which is powered by sensors and diagnostic system installed on vehicles as well as incorporated in infrastructure indicates problems before they arise or become critical [10].

Cybersecurity threats posses a real hazard to autonomous train operations as large amounts of data flow through the train systems and in communication between the train and radio-based communication and control systems. Evidence show that most cyberattacks mostly target ticketing and information systems, CCTVs, onboard Wi-Fi and entertainment systems [11]. Operational technology is not disrupted in the vast majority of recorded cases. On-board equipment as well as trackside systems may be targeted by cyberattacks. Among the current challenges, there is a problem of integration of new systems with legacy systems used, while building resilience to cyber threats. To prevent or mitigate the risks of cyberattacks, study [12] proposes multi-layered security framework with continuous monitoring, use of AI-driven treat detection and robust authentication.

When considering a wide infrastructure, interaction between vehicles (V2V) and vehicles and infrastructure (V2I) need to ensure a safe and efficient operation. The traffic management system (TMS) is a key component in ensuring safe operation of more trains on infrastructure. This system coordinates trains, ensures that only one train at a time can occupy one section, adjust train speed for maximum efficiency, controls adherence to timetable etc [13]. This layer ensures that no collisions occur.

Regulatory and standardization measures include sets of safety standards and regulations to ensure safe operation. European Rail Traffic Management System (ERTMS) is one of the key frameworks of railway standardization, especially in European railway area. ERTMS is composed of European Train Control System (ETCS) and Global System for Mobile Communication – Railways (GSM-R). Its standardised technology enables for interoperability on between different countries. Automatic Train Operation (ATO) is also part of ERTMS [14].

From the operational point of view, a centralised control is preferred. Autonomous operations will be overseen from remote control centres with a possibility of remote control of a train in case of need. As mentioned before, a predictive maintenance approach should be applied to mitigate risks even before they arise. From operational point of view this needs to be taken into account especially in cases of planning inspections and maintenance work and use data-driven approach in both, fleet and infrastructure management.

In case of any emergency event, the operating and safety staff must be ready to handle the situation. Rescue in railway might be very difficult especially at remote locations. Safety drills are necessary to prepare staff for these situations. In case of GoA 4, also education among passengers is very important as the train is unattended in this mode. Remote centres might provide passengers with real time instructions, but a big part of responsibility lays still on their hands.

4 FUTURE PERSPECTIVES

The Europe's Rail project plans to demonstrate autonomous train operation up to Technology Readiness Level ranging from 5 to 7 for different components and aspects [9]. There are still many hurdles to overcome. The technological challenges have been mainly described before. There is however, one more challenge connected to the perception of autonomous technology by the public. Infrastructure is also a big topic. On a greater scale, it will require huge investments in technology and equipment ranging from safety and signalling systems to platforms and stations. When building a new infrastructure, it should be built with future autonomous operation in mind [3]. The autonomous operation will be possible at all types of railway operations such as metro systems, regional lines, light rail systems and even high speed rail systems.

5 CONCLUSION

Autonomous railway operation will surely play a huge role in future. As automation can increase safety and efficiency, while also reducing operating costs, especially in terms of human resources. There are four grades of automation, which might suit different needs. All grades support (or even replace) driver's position. Especially in higher grades of automation a fail safe operation of technical equipment is crucial for hundreds of lives on-board. There are ways, which ensure this is achieved including SIL-4 certification, backups and dual channel systems. Regulatory measures play role in interoperability and universality of systems. Operating staff must be prepared for transition to remote operations and bigger reliance on monitoring remote control technologies.

There are undoubtedly many advantages to autonomous railways, however their research and development faces many challenges and requires significant funding. However, autonomous railway presents a future-proof solution for safe, green and efficient rail transport.

REFERENCES

[1] ZIEGER, Stephan a NIESSEN, Nils. Opportunities and Challenges for the Demand-Responsive Transport Using Highly Automated and Autonomous Rail Units in Rural Areas. Online. *2021 IEEE Intelligent Vehicles Symposium (IV)*. 2021, s. 77-82. ISBN 978-1-7281-5394-0. Dostupné z: https://doi.org/10.1109/IV48863.2021.9575561. [cit. 2025-03-31].

[2] MARINOV, Marin; ŞAHIN, İsmail; RICCI, Stefano a VASIC-FRANKLIN, Gordana. Railway operations, time-tabling and control. Online. *Research in Transportation Economics*. 2013, roč. 41, č. 1, s. 59-75. ISSN 07398859. Dostupné z: https://doi.org/10.1016/j.retrec.2012.10.003. [cit. 2025-03-31].

[3] HITACHI. *Driverless Trains: Past, Present and Future*. Online. HITACHI. 2023. Dostupné z: https://www.hitachirail.com/blog/2023/driverless-trains-past-present-and-future/. [cit. 2025-03-26].

[4] UITP. *Automated metros*. Online. UITP. Uitp.org. Dostupné z: https://www.uitp.org/topics/automated-metros/. [cit. 2025-03-26].

[5] TONK, Abhimanyu; CHELOUATI, Mohammed; BOUSSIF, Abderraouf; BEUGIN, Julie a KOURSI, Miloudi El. A safety assurance methodology for autonomous trains. Online. *Transportation Research Procedia*. 2023, roč. 72, s. 3016-3023. ISSN 23521465. Dostupné z: https://doi.org/10.1016/j.trpro.2023.11.849. [cit. 2025-03-27].

[6] ROSIĆ, Slobodan; STAMENKOVIĆ, Dušan; BANIĆ, Milan; SIMONOVIĆ, Miloš; RISTIĆ-DURRANT, Danijela et al. Analysis of the Safety Level of Obstacle Detection in Autonomous Railway Vehicles. Online. *Acta Polytechnica Hungarica*. 2022, roč. 19, č. 3, s. 187-205. ISSN 17858860. Dostupné z: https://doi.org/10.12700/APH.19.3.2022.3.15. [cit. 2025-03-27].

[7] KOUR, Ravdeep; PATWARDHAN, Amit; THADURI, Adithya a KARIM, Ramin. A review on cybersecurity in railways. Online. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*. 2023, roč. 237, č. 1, s. 3-20. ISSN 0954-4097. Dostupné z: https://doi.org/10.1177/09544097221089389. [cit. 2025-03-27].

[8] PELESKA, Jan; HAXTHAUSEN, Anne E. a LECOMTE, Thierry. Standardisation Considerations for Autonomous Train Control. Online. *Leveraging Applications of Formal Methods, Verification and Validation. Practice*. Lecture Notes in Computer Science. 2022, s. 286-307. ISBN 978-3-031-19761-1. Dostupné z: https://doi.org/10.1007/978-3-031-19762-8_22. [cit. 2025-03-27].

[9] *FP2 – R2DATO*. Online. EUROPE'S RAIL. Europe's Rail. Dostupné z: https://rail-research.europa.eu/rail-projects/fp2-r2dato/. [cit. 2025-03-27].

[10] INTERNATIONAL RAILWAY SAFETY COMMISION. *Advancing Railway Safety: The Role of Technology*. Online. 2023. Dostupné z: https://www.irsc2016.org/advancing-railway-safety-the-role-of-technology/?utm_source=chatgpt.com. [cit. 2025-03-28].

[11] PAWLIK, Marek. Cybersecurity Guidelines for the Employees of the Railway Entities. Online. *Problemy Kolejnictwa - Railway Reports*. 2021, roč. 65, č. 191, s. 95-102. ISSN 2544-9451. Dostupné z: https://doi.org/10.36137/1915E. [cit. 2025-03-28].

[12] IBADAH, Nisrine; BENAVENTE-PECES, César a PAHL, Marc-Oliver. Securing the Future of Railway Systems: A Comprehensive Cybersecurity Strategy for Critical On-Board and Track-Side Infrastructure. Online. *Sensors*. 2024, roč. 24, č. 24. ISSN 1424-8220. Dostupné z: https://doi.org/10.3390/s24248218. [cit. 2025-03-28].

[13] REYES, José A.; QUINTANO, José A.; MATOWICKI, Michal; KAČMAŘÍK, Petr; GURNÍK, Peter et al. EU-Rail FutuRe Project – Innovative CCS

Solutions for Interoperable Regional Lines. Online. *Transport Transitions: Advancing Sustainable and Inclusive Mobility*. Lecture Notes in Mobility. 2025, s. 508-514. ISBN 978-3-031-85577-1. Dostupné z: https://doi.org/10.1007/978-3-031-85578-8_67. [cit. 2025-03-28].

[14] EUROPEAN RAIL TRAFFIC MANAGEMENT SYSTEM. *ERTMS*. Online. Dostupné z: https://www.ertms.net/. [cit. 2025-03-28].

ANALÝZA VÝJAZDOV ZDRAVOTNEJ ZÁCHRANNEJ SLUŽBY NA SLOVENSKU A VÝVOJOVÉ TRENDY

Lukáš Valla[1]

ABSTRAKT

Cieľom tohto článku je analyzovať štatistické údaje o výjazdoch záchrannej zdravotnej služby na Slovensku so zameraním na vývojové trendy v rozdelení posádok. Aktuálne dáta naznačujú klesajúcu potrebu výjazdov rýchlej lekárskej pomoci (RLP) a nárast výjazdov rýchlej zdravotníckej pomoci (RZP), čo možno pripísať širokým kompetenciám zdravotníckych záchranárov v oblasti diagnostiky a terapeutických postupov. Štatistická analýza porovnáva frekvenciu výjazdov posádok RLP a RZP v období 2019 – 2024. Súčasne sa v článku hodnotí spektrum operátorských diagnóz, pri ktorých je na Slovensku najčastejšie vysielaná záchranná zdravotná služba.

Kľúčové slová:
Záchranná zdravotná služba, posádky ZZS, štatistika

ABSTRACT

The aim of this article is to analyse statistical data on ambulance service calls in Slovakia with a focus on development trends in the distribution of crews. Current data indicate a decreasing need for ambulance ambulance ambulance calls and an increase in ambulance ambulance ambulance calls, which can be attributed to the wide competences of paramedics in the field of diagnostics and therapeutic procedures. The statistical analysis compares the frequency of R ambulance and paramedic ambulance crew dispatches in the period 2019-2024. At the same time, the article evaluates the spectrum of operator diagnoses for which the paramedic ambulance service is most frequently dispatched in Slovakia.

Keywords:
Ambulance medical service, ambulance crews, statistics

1 Ing. Lukáš Valla, Univerzitná 8215/1, 010 26 Žilina, lukas.valla@uniza.sk

ÚVOD

Zdravotnícka záchranná služba (ZZS) predstavuje jeden z pilierov neodkladnej zdravotnej starostlivosti a zabezpečuje rýchlu odbornú pomoc pacientom v akútnych stavoch. Na Slovensku fungujú dva základné typy posádok – rýchla lekárska pomoc (RLP), ktorá je tvorená lekárom, záchranárom a vodičom, a rýchla zdravotnícka pomoc (RZP), kde pôsobia dvaja zdravotnícki záchranári a vodič. V posledných rokoch je badať trend poklesu výjazdov RLP a naopak, nárast výjazdov RZP, čo súvisí najmä s rozšírením kompetencií zdravotníckych záchranárov, ako aj s optimalizáciou systému vysielania posádok.

Cieľom tohto článku je analyzovať štatistické údaje o výjazdoch ZZS na Slovensku za obdobie rokov 2019 až 2024, s dôrazom na vývojové trendy v rozdelení medzi RLP a RZP. Výskum sa zameriava na porovnanie výjazdov k vybraným operátorským diagnózam, koreláciu medzi typmi posádok a ich činnosťou, ako aj regresnú analýzu s cieľom predikovať ďalší vývoj. Získané poznatky môžu slúžiť ako podklad pre optimalizáciu systému ZZS a efektívnejšie využívanie ľudských zdrojov v praxi.

1 KORELÁCIA VÝJAZDOV ZZS K VYBRANÝM STAVOM

Na základe údajov o výjazdoch zdravotníckych záchranných služieb typu RLP (posádky s lekárom) a RZP (posádky bez lekára) k vybraným diagnózam za obdobie rokov 2019 až 2024 bola vykonaná korelačná analýza. Cieľom tejto analýzy bolo zistiť, či existuje vzájomný vzťah medzi počtami výjazdov RLP a RZP posádok podľa jednotlivých diagnóz.

Charakteristika použitých údajov:

Analyzovaných bolo spolu **21 najčastejších diagnóz**, pričom každá diagnóza bola vyjadrená dvoma hodnotami:

- Počet výjazdov RLP posádok (s lekárom).
- Počet výjazdov RZP posádok (bez lekára).
- Údaje boli sumarizované za celé obdobie (2019 – 2024).

V článku je spracovaných 21 operátorských diagnóz, ktoré sa považujú za najvýznamnejšie pre výjazd zdravotnej záchrannej služby. V tabuľke 1 sa nachádza krátky popis stavu ku konkrétnej operátorskej diagnóze.

Operátorská diagnóza	Krátky popis stavu
Agresívny pacient	Agresivita môže byť zapríčinená z rôznych dôvodov. Môže to byť vplyv omamných látok, ale aj psychiatrické ochorenia, alebo poruchy kognitívneho vnímania.
Alergická reakcia	Rôzne stupne a závažnosti od vyrážok až po závažné stavy ako anafilaktický šok, vyžadujúci si urgentnú starostlivosť.
ASTMA/CHOCHP	Astma aj chronická obštrukčná choroba pľúc, je celoživotné ochorenie pľúc. Môže mať však akútnu fázu, kedy si pacient vyžaduje neodkladnú urgentnú zdravotnú starostlivosť.
Úraz	Rôzne druhy úrazov od menej závažných ako sú rezné rany, odreniny, tupé poranenia až po závažné ako sú amputácie a polytraumy.
Bezvedomie	Bezvedomie, ale dýcha, je stav pri ktorom došlo k poruche vedomia u pacienta z rôznych príčin.
Dopravná nehoda	Rôzne stavy pacientov. Od zlomenín až po polytraumy. Záleží od mechanizmu dopravnej nehody.
Febrilne kŕče	Stav, ktorý vzniká u malých detí, keď ešte nemajú ustálenú termoreguláciu a ich organizmus sa nevie vyrovnať s teplotou pri zápalových ochoreniach.
Hypertenzia	Ide o stav vysokého tlaku krvi.
Hypotenzia	Stav zníženého krvného tlaku.
Intoxikácia	Otrava rôznymi spôsobmi. Otravy plynom, tekutinou ale aj jedlom. Môže ísť o závažné a menej závažné stavy.
Kŕče a EPI pretrvávajúce	Ide o kŕčovité stavy zapríčinené neobvyklými vzruchmi v mozgu, prejavujúce sa sťahmi svalov.
Kolaps	Laicky povedané ,,odpadnutie“ ide o stav dočasného nedokrvenia mozgu. Organizmus sa po určitej dobe preberie.
NCMP	Náhla cievna mozgová príhoda. Môže mať rôzne formy od ľahkých, kedy môže dochádzať k ochabnutiu končatín, nezrozumiteľnej reči až po vážne stavy, kedy môže vzniknúť až bezvedomie.
Nešpec. bolesti na hrudníku	Môže ísť o infarkt myokardu. Treba urýchlene na adrese točiť EKG záznam pre zhodnotenie stavu pacienta.
Nešpec. dýchacie problémy	Môže ísť o rôzne stavy. Príčinami môžu byť zápaly, astma, alergie...
Status epilepticus	Ide o veľmi vážny stav. Kedy aj po podaní liekov na uvoľnenie kŕčov pacient má stále epilepsiu. Tento stav si vyžaduje uspatie pacienta, intubáciu a urýchlený prevoz do nemocnice.
Stav po záchvate kŕčov	Stav zväčša spojený s epilepsiou, kedy už dozneli kŕče a pacient sa postupne preberá k vedomiu.
Stenokardie	Bolesť na hrudníku. Býva symptómom infarktu myokardu. Okamžite treba natočiť EKG na zistenie stavu srdca.
TANR	Telefonicky asistovaná neodkladná resuscitácia. Rozdiel oproti náhlej zástave obehu je, že svedkovia na základe inštrukcií operátora vykonávajú na adrese resuscitáciu.

Tabuľka 1 Operátorské diagnózy a krátky popis k nim. Zdroj: autor

V ďalšom kroku boli spočítané celkové počty výjazdov RLP a RZP posádok k vybraným stavom za roky 2019 až 2024. Celkové počty sú uvedené v tabuľke 2.5. Zároveň sú zmapované rozdiely v početnosti výjazdov medzi RLP posádkami a RZP posádkami.

P.Č.	OPERATORSKA_DG	RLP	RZP	Rozdiel: RLP-RZP
1	AGRESÍVNY PACIENT	9416	12339	- 2923
2	ALERGICKÁ REAKCIA	9370	14227	- 4857
3	ASTMA/CHOCHP	16451	8927	7524
4	BEZVEDOMIE	67219	24911	42308
5	DOPRAVNÁ NEHODA	18573	34946	- 16373
6	FEBRILNÉ KŔČE	2775	1524	1251
7	HYPERTENZIA	50068	165020	- 114952
8	HYPOTENZIA	1899	17894	- 15995
9	INTOXIKÁCIA	9905	28303	- 18398
10	KOLAPS	42921	96820	- 53899
11	KŔČE/EPI PRETRVÁVAJÚCE	23301	12077	11224
12	NCMP	43321	39843	3478
13	NEŠPEC. BOLESTI NA HRUDNÍKU	5504	55288	- 49784
14	NEŠPEC. DÝCHACIE PROBLÉMY	9814	154077	- 144263
15	NÁHLE ZAST. OBEHU-BEZ TANR/KPR	11439	7943	3496
16	STATUS EPILEPTICUS	983	330	653
17	STAV PO ZÁCHVATE KŔČOV	4245	29229	- 24984
18	STENOKARDIE	83449	39299	- 44150
19	SŤAŽENÉ DÝCHANIE	133674	64315	69359
20	TANR/KPR NÁHLE ZAST. OBEHU	25151	8855	16296
21	ÚRAZ	12527	76734	- 64207
	Celkom výjazdov vo vybraných stavoch:	**582005**	**892906**	**-310901**

Tabuľka 2 Početnosť výjazdov RLP a RZP v rokoch 2019 až 2024. Zdroj: autor

Možnosti hodnotenia korelácie:

- **0,8 až 1**: veľmi silná korelácia
- **0,5 až 0,8**: stredne silná korelácia
- **0,3 až 0,5**: slabá korelácia
- **0 až 0,3**: veľmi slabá alebo žiadna korelácia

Vypočítaný bol Pearsonov korelačný koeficient medzi počtom výjazdov RLP a RZP. Výsledná hodnota korelačného koeficientu je:

r = 0,2538

Táto hodnota predstavuje **slabú pozitívnu koreláciu**.

Pozitívna korelácia znamená, že existuje určitý trend, podľa ktorého diagnózy s vyšším počtom výjazdov RLP majú miernu tendenciu mať aj vyšší počet výjazdov RZP. Avšak vzhľadom na hodnotu koeficientu (0,2538) ide iba o slabú koreláciu. Táto hodnota naznačuje, že síce existuje mierny spoločný trend medzi RLP a RZP výjazdmi, ale vzťah nie je silný. Slabá korelácia zároveň hovorí o tom, že existuje viacero diagnóz, pri ktorých výjazdy RLP a RZP nie sú priamo úmerné. To znamená, že počet výjazdov jedného typu posádky nemožno spoľahlivo odhadnúť len z počtu výjazdov druhého typu posádky.

Slabá korelácia (r = 0,2538) naznačuje, že posádky RLP a RZP zasahujú pri rôznych typoch diagnóz rôznymi spôsobmi. Napríklad niektoré diagnózy sú výrazne častejšie riešené jedným typom posádok (RLP alebo RZP), čo potvrdzujú výrazné rozdiely v údajoch (napríklad Hypertenzia, Kolaps, či Nešpecifické dýchacie problémy). Diagnózy, pri ktorých je vysoký rozdiel medzi RLP a RZP (napr. Stenokardia, Nešpecifické dýchacie problémy, Úrazy), naznačujú, že systém urgentnej starostlivosti sa môže optimalizovať práve zacielením na tieto konkrétne diagnózy (napr. lepšia kategorizácia výjazdov, zmena spôsobu vysielania posádok, posilnenie konkrétneho typu posádky). Tento výsledok naznačuje, že je dôležité skúmať individuálne diagnózy, pretože agregovaná analýza nemusí dostatočne vystihovať špecifické trendy jednotlivých diagnóz.

Zhrnutie:

Korelačný koeficient **r = 0,2538** znamená **slabú pozitívnu koreláciu** medzi počtom výjazdov RLP a RZP posádok podľa diagnóz. Výsledok potvrdzuje, že existuje iba čiastočný, nie príliš silný vzťah medzi týmito dvoma typmi výjazdov. Zároveň naznačuje potrebu detailnejšieho skúmania jednotlivých diagnóz osobitne, aby bolo možné systém efektívnejšie nastaviť a optimalizovať.

2 REGRESIA A PREDIKCIA VÝJAZDOV

Autori sa v nasledujúcej časti pokúsili využiť štatistickú metódu regresie na počet výjazdov za roky 2019 až 2024 a počet posádok kategórie RZP a RLP.

	2019	**2020**	**2021**	**2022**	**2023**	**2024**
RLP	158922	127792	120407	122141	117682	111648
Počet RLP posádok	81	80	80	79	79	81
RZP	381770	355470	369064	363958	367277	376703
Počet RZP posádok	187	188	188	191	191	191
Celkový počet výjazdov	540692	483262	489471	486099	484959	488351

Tabuľka 3 Vstupné údaje pre regresiu. Zdroj: autor

Lineárna regresia: Výjazdy RLP podľa počtu RLP posádok

Ako vstupné údaje sú využité dáta z rokov 2019 – 2024:

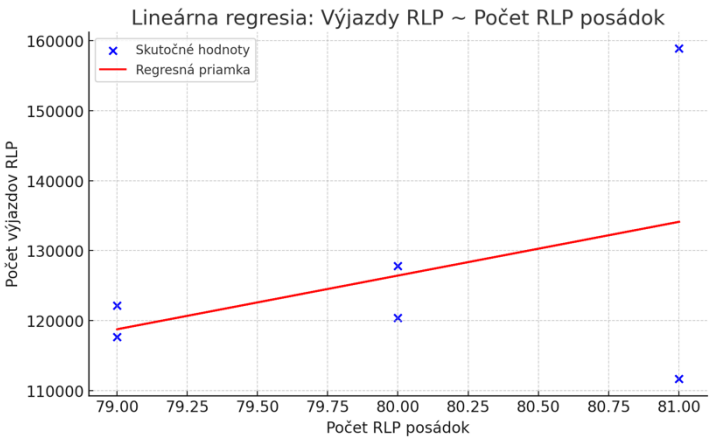
- **Nezávislá premenná (X):** počet RLP posádok
- **Závislá premenná (y):** počet výjazdov RLP

Použitie lineárnej regresie:

Výjazdy RLP = β_0 **+** β_1 *** Počet posádok RLP**

Výsledky modelu:

- **Smernica (sklon):** β_1= približne **1798** - ak sa počet RLP posádok zvýši o 1, očakáva sa zvýšenie počtu výjazdov v priemere o 1798.
- **Y-priesečník (konštanta):** β_0 = približne **-19765**
- **R² (koeficient determinácie):** ≈ 0.88 model vysvetľuje **88 % variability** vo výjazdoch. To je silná závislosť.



Graf 1 Lineárna regresia: výjazdy RLP. Zdroj: autor

Lineárna regresia: Výjazdy RZP podľa počtu RZP posádok

Ako vstupné údaje sú opäť využité dáta z rokov 2019 – 2024:

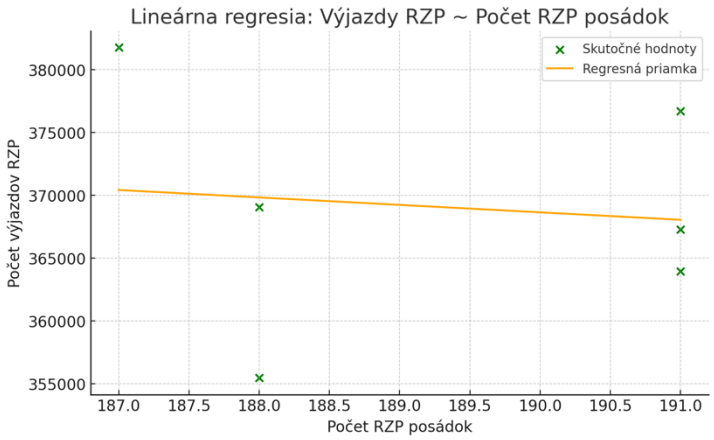
- **Nezávislá premenná (X):** počet RZP posádok
- **Závislá premenná (y):** počet výjazdov RZP

Po využití rovnakého typu lineárnej regresie:

Výjazdy RZP = β_0 **+** β_1 *** Počet posádok RZP**

Výsledky modelu:

- **Smernica (sklon):** β_1 = približne **1903** - ak sa počet RZP posádok zvýši o 1, očakáva sa zvýšenie výjazdov v priemere o 1903.
- **Y-priesečník (konštanta):** β_0 = približne **16356**
- **R² (koeficient determinácie):** ≈ 0.84 - model vysvetľuje **84 % variability**, čo naznačuje veľmi silnú závislosť.



Graf 2 Lineárna regresia: výjazdy RZP. Zdroj: autor

V ďalšej časti je realizovaná predikcia vývoja počtu výjazdov jednotlivých posádok v horizonte najbližších 10 rokov s očakávaným ďalším znížením počtu posádok typu RLP a nárast počtu posádok RZP. S tým súvisí aj zmena celkového počtu výjazdov každého druhu z posádok.

	Rok	RLP posádky	RLP výjazdy	RZP posádky	RZP výjazdy
0	2025	81	127391	191	370639
1	2026	80	126325	194	373838
2	2027	79	125259	198	377036
3	2028	78	124193	201	380234
4	2029	77	123127	204	383432
5	2030	75	122061	208	386630
6	2031	74	120995	211	389828
7	2032	73	119929	214	393027
8	2033	72	118863	218	396225
9	2034	71	117797	221	399423

Tabuľka 4 Predikcia vývoja počtu výjazdov. Zdroj: autor

ZÁVER

Analýza výjazdov zdravotníckej záchrannej služby na Slovensku v období rokov 2019 až 2024 poukázala na zreteľný trend znižovania počtu výjazdov posádok RLP a súčasný nárast zásahov RZP. Korelačná analýza medzi počtami výjazdov RLP a RZP k vybraným operátorským diagnózam odhalila len slabú pozitívnu koreláciu (r = 0,2538), čo naznačuje, že tieto dva typy posádok zasahujú pri rôznych typoch prípadov s odlišnou frekvenciou. Tento fakt podporuje potrebu analyzovať výjazdy individuálne podľa diagnóz, keďže agregované údaje nemusia presne vystihovať realitu. Regresná analýza zároveň ukázala silnú závislosť medzi počtom posádok a počtom výjazdov, čo umožnilo vytvoriť predikčný model vývoja do roku 2034. Model predpokladá postupný pokles výjazdov RLP a nárast výjazdov RZP, čo korešponduje s aktuálnymi trendmi a smerovaním systému prednemocničnej starostlivosti. Výsledky tejto štúdie potvrdzujú význam pokračujúcej racionalizácie a efektívnejšieho rozdelenia výjazdových posádok, čo môže viesť k vyššej flexibilite a kvalite poskytovanej urgentnej zdravotnej starostlivosti.

POĎAKOVANIE

Článok vznikol s podporou projektu KEGA 035ŽU-4/2025 Inovatívne modulárne vzdelávacie kurzy ako efektívny nástroj na zvýšenie bezpečnosti na školách.

Touto cestou by som sa zároveň chcel poďakovať vedeniu Operačného strediska 155 za poskytnuté dáta, vďaka ktorým mohol vzniknúť tento článok aj ďalší výskum v oblasti zdravotnej záchrannej služby.

LITERATÚRA

[1] **ISIBALO.** *Korelace (MAT – Statistika).* 2020. Youtube video. [online]. [cit. 2025-04-01]. Dostupné na: https://www.youtube.com/watch?v=CLXb-4nYLeQ

[2] **FIŘTOVÁ, L.** *Korelace – co to je korelace a co znamená korelační koeficient*. ČR : ExcelTower, 2021. [online]. [cit. 2025-04-01]. Dostupné na: https://exceltown.com/navody/pokrocila-analyza-regrese-korelace/korelace-co-to-vlastne-je/

[3] **CHATTERJEE, S., HADI, A**. *Regresion analysis by example*. USA : WILEY, 2012. ISBN: 878-0-480-90584-5. [online]. [cit. 2025-04-01]. Dostupné na: https://www.google.com/books?hl=sk&lr=&id=zyjWBgAAQBAJ&oi=fnd&pg=PP1&dq=regression&ots=O-eBcN1TgY&sig=0bBgzKTQUbz3Nnn6j3HsUA4VfnU

[4] **KOS 155.** *Výjazdy zdravotnej záchrannej služby SR v rokoch 2019 až 2024.* Bratislava : KOS 155, 2025. Interné dokumenty. Dostupné pre autora s povolením publikovať výsledky.

MOŽNOSTI ZVÝŠENÍ ÚROVNĚ ZABEZPEČENÍ BUDOV MĚSTSKÝCH ÚŘADŮ PŘED HROZBOU ÚTOKU AKTIVNÍHO STŘELCE

Ondřej Velísek[1]

ABSTRAKT

Při zvyšování úrovně zabezpečení a zajišťování ochrany tzv. měkkých cílů je zásadní vycházet z provedeného posouzení relevantních rizik a zohlednit rovněž funkci daného objektu. Tyto aspekty jsou do značné míry závislé na typu konkrétního měkkého cíle a jejich zodolnění proto vyžaduje hledání specifického řešení pro každý typ měkkého cíle. Příspěvek se zabývá problematikou ochrany měkkých cílů, se zvláštním důrazem na úřady a administrativní budovy. Zohledňuje specifika těchto míst, kde je nutné nalézt rovnováhu mezi otevřeností a dostupností úřadu pro veřejnost a zajištěním bezpečnosti zaměstnanců a návštěvníků.

Klíčová slova:
Měkké cíle, Aktivní střelec, Rizika, Bezpečnost

ABSTRACT

When increasing the level of security and ensuring the protection of so-called soft targets, it is essential to proceed from the relevant risk assessment and also take into account the function of the given object. These aspects are largely dependent on the type of specific soft target and their strengthening therefore requires finding a specific solution for each type of soft target. The paper deals with the issue of protecting soft targets, with a special emphasis on offices and administrative buildings. It takes into account the specifics of these places, where it is necessary to find a balance between the openness and accessibility of the office to the public and ensuring the safety of employees and visitors.

Key words:
Soft Targets, Active shooter, Risks, Security

1 Univerzita Tomáše Bati ve Zlíně, Nad Stráněmi 4511, 760 05 Zlín, o_velisek@utb.cz,

1 ÚVOD

V době, kdy celosvětově narůstá počet násilných incidentů na veřejných místech, stává se ochrana měkkých cílů jednou z klíčových bezpečnostních výzev 21. století. Tragické případy se nestávají jen v zahraničí, ale již také v České republice. Střelba na Filozofické fakultě Univerzity Karlovy v prosinci 2023, útok v nemocnici v Ostravě na konci roku 2019 či události na začátku roku 2015 v restauraci v Uherském Brodě, jasně demonstrují zranitelnost míst, kde se shromažďují lidé a která jsou bez výrazných bezpečnostních opatření.

Ochrana měkkých cílů představuje mimořádně složitou výzvu, protože vyžaduje nalezení křehké rovnováhy mezi potřebou zajistit bezpečnost a zároveň zachovat otevřenost a funkčnost těchto prostorů. Nelze jednoduše aplikovat metody používané při ochraně vojenských či vládních objektů – škola nemůže fungovat jako pevnost, nemocnice či úřady musí zůstat snadno přístupné a kulturní zařízení nemohou ztrácet svůj přívětivý charakter.

Přesná definice měkkého cíle (tzv. „soft targets“) která by byla všeobecně přijímána, prozatím neexistuje. Koncepce ochrany měkkých cílů pro roky 2017–2020 vydané Ministerstvem vnitra [1] označuje měkké cíle jako „objekty, prostory nebo akce charakterizované častou přítomností většího počtu osob a současně absencí, či nízkou úrovní zabezpečení proti násilným útokům.“ Pro americkou federální agenturu Cybersecure and infrastructure security agency (agentura pro kybernetickou a infrastrukturní bezpečnost) jsou měkké cíle obvykle definované jako místa nebo prostředí, která jsou snadno dostupná a přitahují velké množství lidí, a zároveň mohou být lehce zranitelná vůči útokům [2].

V mnoha publikacích se také můžeme setkat s návazným pojmem „crowded places“ (volně přeloženo jako přeplněná místa). Dle australské strategie pro ochranu přeplněných míst před terorismem [3] jsou přeplněné místa taková místa, která jsou snadno dostupná velkému počtu lidí a která jsou atraktivní pro cíl útoku. Tato místa nemusí být nutně přeplněné vždy, počet lidí se může měnit dle ročního období, kulturních akcí či během dne a noci. S touto definicí se také ztotožňuje novozélandská strategie o ochraně přeplněných míst před útokem [4].

Mezi měkké cíle, a zároveň přeplněná místa, můžeme řadit například školy, nákupní centra, divadla, hotely, úřady, restaurace, kulturní akce, náboženské akce, nemocnice, parky, sportovní stadiony, veřejnou dopravu atd. [1,5,6].

Jak již bylo zmíněno v úvodu článku, problematika útoků aktivního střelce na měkké cíle se netýká jen zahraničí, ale také České republiky. Policie České republiky označuje aktivního střelce jako nebezpečného ozbrojeného pachatele, jehož cílem je zabít co největší počet lidí, a to v době, než bude jeho

čin ukončen policií nebo vlastní sebevraždou. Útok je zpravidla dlouhodobě plánován a je promyšlený. Pachatel nemívá připravený plán ústupu, nemá zájem o vyjednávání a také se nehodlá v žádném případě vzdát [7].

Definice aktivního střelce dle U.S. Department of Homeland Security (Ministerstvo vnitřní bezpečnosti Spojených států amerických) vymezuje aktivního střelce jako jedince, který je aktivně zapojen do usmrcení či pokusu o zabití co nejvíce lidí v uzavřeném a přelidněném prostoru. Ve většině případů aktivní střelec využije pro svůj čin střelnou zbraň. Pro jeho čin neexistuje vzorec ani metoda výběru obětí. Situace kolem aktivního střelce jsou nepředvídatelné a vyvíjí se velmi rychle. Typicky je vyžadován okamžitý zásah bezpečnostních složek, aby byl útok zastaven a byla minimalizována škoda způsobená obětem [8].

Městský úřad náleží do kategorie měkkých cílů a také je potenciálních cílem pro útok aktivního střelce. Městský úřad je jakožto orgán města definován v zákoně č 128/2000Sb. O obcích [9]. Zde je také potřeba vymezit městské úřady, které pro potenciálního aktivního střelce připadají nejvíce v úvahu. Útočník má za cíl usmrcení co největšího počtu lidí. Z toho důvodu bude nejpravděpodobněji vyhledávat na úřadě místa, kde se lidé nejčastěji shlukují. Mezi tato místa můžeme řadit agendu cestovních a osobních dokladů, agendu vozidel a řidičských oprávnění agendu živností apod. Tuto agendu zpracovávají tzv. obecní úřady s rozšířenou působností. Tyto úřady kromě přenesené působnosti v základním rozsahu a přenesené působnosti pověřených obecních úřadů vykonávají také další přenesenou působnost, a to ve svěřeném rozsahu ve správním obvodu určené příslušným prováděcím předpisem (vždy se jedná o více obcí). Rozšířená působnost je věcně vymezena v mnoha speciálních zákonech, včetně zákona o obcích [10]. Všech 205 obcí s rozšířenou působností v České republice jsou zároveň městy. Proto také obecní úřady s rozšířenou působností jsou jejich městské úřady případně magistráty [11]

2 OCHRANA MĚKKÝCH CÍLU V ČESKÉ REPUBLICE

V návaznosti na zhoršení bezpečnostní situace v Evropě po roce 2014 a s ohledem na rostoucí hrozbu terorismu, se Česká republika zaměřila na problematiku ochrany měkkých cílů. Vytvořením a přijetím nových koncepčních materiálů významně rozšířila stávající *Strategii pro boj proti terorismu* z roku 2013 [12]

Bezpečnostní strategie z roku 2015 představuje logické pokračování dřívějších koncepčních materiálů v oblasti bezpečnosti. Jako stěžejní dokument definuje základní hodnoty a zájmy státu, analyzuje bezpečnostní prostředí a formuluje dlouhodobou strategii pro jejich ochranu [13]. Na tento dokument navazuje *Bezpečnostní strategie České republiky* z roku 2023. Ten představuje ústřední dokument bezpečnostní politiky státu. Vycházejí z ní veškeré další strategie a koncepce v této oblasti. Strategie vymezuje základní principy a

směřování bezpečnostní politiky a je závazná pro všechny státní orgány a veřejnou správu. Slouží jako podklad pro strategická rozhodnutí na všech úrovních bezpečnostního systému a její realizace je pravidelně vyhodnocována [14].

Neméně významným dokumentem je *Audit národní bezpečnosti* z roku 2016. Ten se komplexně zabývá širokým spektrem hrozeb a rizik pro Českou republiku v souvislosti s globálními bezpečnostními výzvami. Důkladně analyzuje hrozbu terorismu, včetně útoků na měkké cíle, a navrhuje preventivní opatření [15]. V roce 2016 byl také přijat *Akční plán pro boj proti terorismu na léta 2016 až 2018*. Tento akční plán se skládá ze tří samostatných dokumentů:

a) Legislativní návrhy v oblasti vnitřní bezpečnosti
b) Protiteroristický balíček (utajovaný vládní dokument)
c) Návrh opatření ke zvýšení bezpečnosti na mezinárodních letištích v ČR [16]

Ministerstvo vnitra vypracovalo také několik nelegislativních dokumentů, které je, s ohledem na danou problematiku, vhodné zmínit. Jedná se o:

- *Základy ochrany měkkých cílů: metodika* [17]
- *Koncepce ochrany měkkých cílů pro roky 2017-2020* [1]
- *Vyhodnocení ohroženosti měkkého cíle* [18]
- *Bezpečnostní standardy pro pořadatele letních sportovních, kulturních a společenských akcí* [19]
- *Bezpečnostní plán měkkého cíle* [20]

Nicméně například dle Benedikta Vangeliho nejsou v České republice důvody pro právní regulaci ochrany měkkých cílů. Právní regulace by dle něj postrádala racionální důvody pro svou existenci a také by nebyla schopna logicky určit komu a jaké povinnosti ukládat. Taková regulace by přinesla pouze zmatek a nerovnost mezi různými subjekty v oblasti práv a povinností. Také by přidělala práci těm, kteří se ochraně měkkých cílů zabývají či ji zajišťují. Podle Vengeliho je vhodné nadále prosazovat dobrovolnou cestu a motivovat měkké cíle ke svému zodolnění a to metodickou a dotační cestou, tak jako je tomu doposud [21].

3 MOŽNOSTI APLIKACE BEZPEČNOSTNÍCH OPATŘENÍ V RÁMCI MĚSTSKÝCH ÚŘADŮ

Jak již bylo zmíněno v předchozí kapitole, v České republice bylo vytvořeno několik dokumentů týkající se problematiky ochrany měkkých cílů. Většina těchto dokumentů se zaměřuje na obecné principy a postupy pokrytí ochrany těchto objektů. Tato kapitola je věnována dokumentu *Základy ochrany*

měkkých cílů: metodika na konkrétní měkký cíl, a to městské úřady, a konkrétní hrozbu, totiž aktivního střelce.

Základy ochrany měkkých cílů: metodika třídí bezpečnostní opatření do tří základních kategorií bezpečnostního systému, a to:

1. fyzická bezpečnost
2. elektronické prvky
3. mechanické prvky

Při výběru bezpečnostního prvku není nejpodstatnější jeho kvalita, nýbrž jeho účelnost a napojení na ostatní prvky bezpečnostního systému. Důležitým aspektem je také to, kdo daný prvek bude zabezpečovat, jak v tom bude proškolen a kontrolován [13].

3.1 FYZICKÁ BEZPEČNOST

Zmíněná metodika rozlišuje v rámci fyzické bezpečnosti dva prvky, a to bezpečnostní pracovníci a ostatní personál. Bezpečnostní pracovníci, ať už zaměstnanci daného subjektu nebo externí firmy, jsou jedním z nejefektivnějších bezpečnostních prvků. Kvalitně vyškolená fyzická ochrana působí nejenom preventivně jako odstrašení, ale při incidentu může zamezit větším ztrátám na životech buď včasnou detekcí hrozby či přímo danou hrozbu odstranit. Ostatním personálem se rozumí pracovníci daného subjektu, jejíchž agenda se nevztahuje přímo na bezpečnost objektu, ve kterém působí, ale mohou se na bezpečnosti podílet [17].

Oba prvky fyzické bezpečnosti mohou zvýšit úroveň zabezpečení městských úřadů před hrozbou útoku aktivního střelce. Personál, který přímo nezodpovídá za bezpečnost může být pravidelně proškolován, jak se při mimořádné události chovat, čímž může zachránit život nejenom sobě, ale i lidem v blízkosti. Bezpečnostní pracovníci jsou velmi efektivním prvkem ochrany, pokud mají dobře nastavená pravidla fungování a jsou správně stanoveny jejich pravomoci. Při špatném nastavení mohou být tito pracovníci pouze finanční zátěž bez reálného přínosu pro bezpečnost měkkého cíle.

3.2 ELEKTRONICKÉ PRVKY

Mezi elektronické prvky v rámci metodiky jsou zmíněny kamerové systémy, poplachové zabezpečovací a tísňové systémy, dohledové a poplachové přijímací centrum, vnitřní rozhlas, rentgen, detektor kovů, detektory výbušnin, přístupové a docházkové systémy, čtečky dokladů, systémy šíření varování a osvětlení [17].

Elektronické prvky, které mohou zvýšit úroveň zabezpečení budov městských úřadů před hrozbou aktivního střelce můžeme zařadit kamerový systém spolu s dohledovým a poplachovým přijímacím centrem. Díky dobře

nastaveným kamerám a správně vyškolenému personálu lze včas detekovat případnou hrozbu a rychle reagovat na hrozící či právě probíhající nebezpečí a tím zamezit dalším ztrátám na životech. S tím také souvisí systémy šíření varování a vnitřní rozhlas. Tyto systémy mohou být využity jako důležitý informační zdroj, který umožňuje včasnou reakci na hrozící či již probíhající útok aktivního střelce.

Naopak mezi prvky elektronické ochrany, které mohou zvýšit úroveň zabezpečení, avšak proti aktivnímu střelci na úřadech nejsou efektivní, řadíme poplachové zabezpečovací a tísňové systémy spolu s osvětlením. Tyto systému slouží k narušení perimetru případně nežádoucímu vstupu do objektu. Z důvodu principu otevřenosti a otvíracích hodin městských úřadů postrádají tyto systémy smysl. Rentgen a detektory kovů případně výbušnin jsou neefektivními prvky ze stejného důvodu. Je snaha co nejrychleji občana odbavit a tyto prvky prodlužují čas strávený na úřadě. Stejně tak přístupové a docházkové systémy, případně čtečky dokladů, mohou způsobit zdržování občanů a neefektivnost městského úřadu.

3.3 MECHANICKÉ PRVKY

Prvky mechanické ochrany jsou bezpečnostní dveře, bezpečnostní okna, ploty, turnikety či sloupky a betonové bloky [17]. Tyto prvky slouží k omezení případě i úplnému znepřístupnění určité cesty. Většina těchto prvků lze použít pro zamezení vstupu aktivního střelce na místa, kde působí zaměstnanci městského úřadu. V případě, že to systém umožňuje, také zabránit aktivnímu střelci v pokračování útoku tím, že se mu zablokují odchozí cesty v daném místě. Sloupky a betonové bloky lze také využít pro znemožnění využití auta jakožto blokády pro únikové cesty.

3.4 DISKUZE

Ochrana městských úřadů jako měkkých cílů proti aktivnímu střelci představuje komplexní bezpečnostní výzvu, která vyžaduje vyvážený přístup mezi zajištěním bezpečnosti a zachováním otevřenosti veřejné instituce.

Domnívám se, že ne všechna standardně doporučovaná bezpečnostní opatření jsou v kontextu městských úřadů stejně efektivní. Zatímco některé prvky mohou významně přispět k prevenci a zmírnění následků potenciálního útoku, jiné mohou narušit základní funkce úřadu nebo vytvářet falešný pocit bezpečí bez reálného přínosu.

Z mého pohledu vyplývá potřeba individualizovaného přístupu k zabezpečení, který zohledňuje specifické charakteristiky konkrétního úřadu – jeho velikost, dispozici, frekvenci návštěvníků a místní bezpečnostní situaci. Univerzální aplikace všech doporučení bez zvážení těchto faktorů může vést k neefektivnímu vynakládání zdrojů.

Pro další rozvoj bezpečnostních strategií je zásadní pravidelné vyhodnocování účinnosti implementovaných opatření, simulační cvičení a sdílení zkušeností mezi jednotlivými úřady. Bezpečnostní systém by měl být dostatečně adaptabilní, aby reagoval na nové hrozby a zároveň naplňoval společenskou funkci městských úřadů jako otevřených a přístupných institucí.

Tato problematika tak otevírá širší diskusi o rovnováze mezi bezpečností a otevřeností ve veřejném prostoru a poukazuje na nutnost zapojení nejen bezpečnostních expertů, ale i zástupců veřejné správy a občanů do formulování bezpečnostních politik.

Významnou dimenzí, je finanční stránka implementace bezpečnostních opatření. Zajištění komplexní ochrany městských úřadů představuje nezanedbatelnou položku v rozpočtech měst, přičemž efektivita vynaložených prostředků není vždy zaručena. Investice do fyzické bezpečnosti, zejména kvalifikovaného personálu, zahrnují nejen přímé mzdové náklady, ale i výdaje na pravidelné školení a psychologickou přípravu. Elektronické bezpečnostní prvky vyžadují kromě počátečních investic také prostředky na pravidelnou údržbu, aktualizace a případné modernizace systémů v reakci na nové bezpečnostní výzvy.

V kontextu omezených rozpočtů samospráv je proto nezbytné přistupovat k bezpečnostním investicím strategicky. Ideálním postupem se jeví důkladné vyhodnocení ohroženosti konkrétního úřadu a následná aplikace takových opatření, která poskytnou optimální poměr mezi vynaloženými prostředky a dosaženou úrovní zabezpečení. Určitou možností pro zmírnění finanční zátěže mohou být dotační programy na ochranu měkkých cílů poskytované státem nebo sdílení nákladů na některé bezpečnostní prvky mezi více subjekty veřejné správy.

Je však třeba zdůraznit, že finanční aspekty by neměly být jediným kritériem při rozhodování o bezpečnostních opatřeních. Hodnota lidských životů a společenské náklady spojené s případným útokem dalece převyšují přímé investice do prevence. Zároveň je nutné průběžně vyhodnocovat účinnost implementovaných opatření a flexibilně reagovat na měnící se bezpečnostní prostředí.

4 ZÁVĚR

V kontextu dokumentu *Základy ochrany měkkých cílů: metodika* bylo zjištěno, že ne všechna standardně doporučovaná bezpečnostní opatření jsou stejně efektivní v prostředí městských úřadů. Za nejúčinnější prvky lze považovat proškolený personál, bezpečnostní pracovníky s jasně definovanými pravomocemi, vhodně nastavené kamerové systémy s dohledovým centrem

a systémy šíření varování. Naopak některé elektronické prvky jako rentgeny či detektory kovů se jeví jako problematické z hlediska plynulosti provozu úřadu.

Přístup k ochraně městských úřadů jako měkkých cílů by měl být vždy individualizovaný, zohledňující specifika konkrétní instituce, místní bezpečnostní situaci a dostupné finanční i personální zdroje. Pouze takový přístup může vést k vytvoření skutečně efektivního bezpečnostního systému, který ochrání návštěvníky i zaměstnance úřadů, aniž by narušil základní funkce těchto institucí jako center veřejné služby přístupných všem občanům.

LITERATURA

[1] MINISTERSTVO VNITRA ČR. *Koncepce ochrany měkkých cílů pro roky 2017-2020* [online]. Praha: MV ČR, 2017 [cit. 2025-03-19]

[2] CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, *Security of Soft Targets and Crowded Places–Resource Guide* [online], 2019, [cit. 2025-03-19] dostupné z: https://www.fema.gov/sites/default/files/2020-03/fema_faith-communities_security-soft-targets-crowded-places.pdf

[3] TASMANIA POLICE. *Australias strategy for protecting crowded places from terrorism* [online]. 2023. [cit. 2025-03-19]. Dostupné z: https://www.police.tas.gov.au/what-we-do/special-response-counter-terrorism/australias-strategy-protecting-crowded-places-terrorism/

[4] NEW ZEALAND GOVERNMENT. *Protecting Our Crowded Places from Attack: New Zealand's Strategy* [online]. 2020. [cit. 2025-03-19]. Dostupné z: https://www.police.govt.nz/advice-services/protecting-crowded-places-attack/crowded-places-strategy

[5] AMERICA´S CYBER DEFENSE AGENCY. *Securing Public Gatherings*. [online], [cit. 2025-03-20] Dostupné z: https://www.cisa.gov/topics/physical-security/securing-public-gatherings.

[6] HOLLYWOOD, John S.; GIERLACK, Keith; MOORE, Pauline; GOODE, Thomas; WILLIS, Henry H. et al. *Improving the Security of Soft Targets and Crowded Places*. REND, 2024. ISBN 10 197741261-0

[7] POLICIE ČESKÉ REPUBLIKY. *Taktické cvičení AMOK – AKTIVNÍ STŘELEC*. Online. 2017. Dostupné z: https://policie.gov.cz/clanek/takticke-cviceni-amok-aktivni-strelec.aspx. [cit. 2025-03-25].

[8] U.S. DEPARMENT OF HOMELAND SECURITY. *Active Shooter How to Respond*. Online. Říjen 2008. Dostupné

z: https://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf. [cit. 2025-03-25].

[9] ČESKO, 2000. Zákon č. 128/2000 Sb., Zákon o obcích (obecní zřízení). In: *Sbírka zákonů České republiky* [online]. [cit. 2025-03-30].Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-128

[10] MINISTERSTVO VNITRA, 2018. *Metodické doporučení k činnosti územních správních celků* [online]. Odbor veřejné správy, dozoru a kontroly. [cit. 2025-03-30]. Dostupné z: https://www.mv.gov./odk2/clanek/metodicke-materialy-k-zakonnym-zmocnenim.aspx

[11] PORTÁL VEŘEJNÉ SPRÁVY, 2025. *Rejstřík orgánů veřejné moci* [online]. [cit. 2025-03-30].Dostupné z: https://portal.gov.cz/organy-verejne-moci/?razeni=&ovm_kod_kategorie=KO11&ovm_kod_pravni_formy=@page=11

[12] MINISTERSTVO VNITRA ČR. *Strategie České republiky pro boj proti terorismu* [online].Praha: MZV ČR, 2013 [cit. 2025-03-30].

[13] MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČR. Bezpečnostní strategie České republiky [online]. In: Praha: MZV ČR, 2015 [cit. 2025-3-31]. ISBN 978-80-7441-005-5

[14] MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČR. Bezpečnostní strategie České republiky [online]. Praha: MZV ČR, 2023 [cit. 2025-03-31].

[15] MINISTERSTVO VNITRA ČR. *Audit národní bezpečnosti* [online]. Praha: MV ČR, 2016 [cit. 2025-03-31]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf

[16] MINISTERSTVO VNITRA – CENTRUM PROTI HYBRIDNÍM HROZBÁM, *Akční plán pro boj proti terorismu pro léta 2016 až 2018*. Centrum proti hybridním hrozbám [online]. Praha: Ministerstvo vnitra [cit. 2025-03-31]. Dostupné z: https://www.mvcr.cz/chh/clanek/akcni-plan-pro-boj-proti-terorismu-proleta-2016-az-2018.aspx

[17] MINISTERSTVO VNITRA ČR. *Základy ochrany měkkých cílů: metodika* [online]. Praha: MV ČR, 2016 [cit. 2025-03-31]

[18] MINISTERSTVO VNITRA – CENTRUM PROTI HYBRIDNÍM HROZBÁM, *Vyhodnocení ohroženosti měkkého cíle.* Centrum proti hybridním hrozbám [online]. Praha: Ministerstvo vnitra. 2017 [cit. 2025-03-31]. Dostupné

z: https://www.mvcr.cz/chh/clanek/vyhodnoceni-ohrozenosti-mekkeho-cile-metodika-ke-stazeni.aspx

[19] MINISTERSTVO VNITRA – CENTRUM PROTI HYBRIDNÍM HROZBÁM, *Bezpečnostní standardy pro pořadatele letních sportovních, kulturních a společenských akcí.* Centrum proti hybridním hrozbám [online]. Praha: Ministerstvo vnitra 2019 [cit. 2025-03-31]. Dostupné z: https://www.mvcr.cz/chh/clanek/terorismus-web-dokumenty-dokumenty.aspx

[20] MINISTERSTVO VNITRA – CENTRUM PROTI HYBRIDNÍM HROZBÁM, *Bezpečnostní plán měkkého cíle.* Centrum proti hybridním hrozbám [online]. Praha: Ministerstvo vnitra [cit. 2025-03-31]. Dostupné z: https://www.mvcr.cz/chh/clanek/terorismus-web-dokumenty-dokumenty.aspx

[21] VANGELI, Benedikt. Právní úprava měkkých cílů v ČR. In: Apelauter a spol. *Ochrana měkkých cílů.* Leges, 2019, ISBN 978-80-7502-427-5