SLOVENSKÁ TECHNICKÁ UNIVERZITA
MATERIÁLOVOTECHNOLOGICKÁ FAKULTA

Ing. Denis Benka

Autoreferát dizertačnej práce

Využitie metód strojového učenia pri analýze stochastických signálov pre potreby riadenia procesov

na získanie akademického titulu doktor („philosophiae doctor“, v skratke „PhD.“)

v doktorandskom študijnom programe: 2621 Automatizácia a informatizácia procesov

v študijnom odbore: kybernetika

Forma štúdia: denná

Trnava, 15.01.2025

STU

Dizertačná práca bola vypracovaná na:
Ústave aplikovanej informatiky, automatizácie a mechatroniky,
Materiálovotechnologickej fakulty so sídlom v Trnave,
Slovenskej Technickej Univerzity v Bratislave

Predkladateľ: **Ing. Denis Benka**
Ústav aplikovanej informatiky, automatizácie a mechatroniky,
Materiálovotechnologická fakulta so sídlom v Trnave
Slovenská technická univerzita v Bratislave
Jána Bottu 2781/25
917 24 Trnava

Školiteľ: **doc. Ing. Gabriel Gašpar, PhD.**
Ústav aplikovanej informatiky, automatizácie a mechatroniky,
Materiálovotechnologická fakulta so sídlom v Trnave
Slovenská technická univerzita v Bratislave
Jána Bottu 2781/25
917 24 Trnava

Autoreferát bol rozoslaný .....

Obhajoba dizertačnej práce sa bude konať dňa.....o.....hod. na Materiálovotechnologickej fakulte so sídlom v Trnave, Slovenskej Technickej Univerzity v Bratislave

.....
prof. Ing. Miloš Čambál, CSc.
dekan Materiálovotechnologickej fakulty STU

STU

SÚHRN

BENKA, Denis: Využitie metód strojového učenia pri analýze stochastických signálov pre potreby riadenia procesov. [Dizertačná práca] - Slovenská technická univerzita v Bratislave. Materiálovotechnologická fakulta; Ústav aplikovanej informatiky, automatizácie a mechatroniky. – Vedúci diplomovej práce: doc. Ing. Gabriel Gašpar, PhD. - Trnava: MTF STU, 2025.

Dizertačná práca sa zaoberá detekciou anomálií v komunikácii priemyselných riadiacich systémov pomocou pokročilých metód strojového učenia. Skúma bezpečnosť a integritu dátových prenosov medzi programovateľnými logickými automatmi, ktoré sú kľúčové pre automatizáciu priemyselných procesov. Cieľom práce bolo navrhnúť metódy schopné efektívne identifikovať kybernetické hrozby a anomálie v reálnom čase.
Práca zahŕňa tvorbu robustného datasetu z reálnej aj simulovanej komunikácie medzi PLC, pričom boli analyzované normálne aj anomálne scenáre. Optimalizácia architektúry a výber hyperparametrov algoritmov strojového učenia zabezpečili maximálnu výkonnosť a minimálny počet falošných detekcií.
Hlavným prínosom je návrh systému pre detekciu anomálií v reálnom čase, ktorý je vhodný pre komplexné priemyselné prostredia. Výsledky otvárajú možnosti ďalšieho výskumu v oblasti hybridných modelov a adaptívnych systémov na zvládanie dynamických hrozieb.

Kľúčové slová: Detekcia anomálie, strojové učenie, kybernetický útok, programovateľné logické automaty

STU

ABSTRACT

BENKA, Denis: Utilization of machine learning methods in the analysis of stochastic signals for process control. [Dissertation thesis] - Slovak University of Technology in Bratislava. Faculty of Materials Science and Technology; Institute of Applied Informatics, Automation, and Mechatronics. – Supervisor: doc. Ing. Gabriel Gašpar, PhD. - Trnava: MTF STU, 2025.

The dissertation focuses on detecting anomalies in industrial control system (ICS) communication using advanced machine learning methods. It examines the security and integrity of data transfers between programmable logic controllers (PLCs), essential for industrial automation. The primary goal was to design methods capable of real-time detection of cybersecurity threats and anomalies.

The research involved developing a robust dataset from real and simulated PLC communication, analyzing both normal and anomalous scenarios. Optimizing algorithm architecture and selecting hyperparameters ensured high performance with minimal false detections.

The main contribution is a real-time anomaly detection system tailored for complex industrial environments. The results highlight opportunities for further research into hybrid and adaptive systems to address dynamic threats.

Keywords: Anomaly detection, machine learning, cyber attack, programmable logic controllers

STU

OBSAH

STU

ÚVOD

Dáta sú základným prvkom mnohých vedeckých a technologických odvetví, pričom inteligentné riadiace systémy (ICS) zohrávajú kľúčovú úlohu v prevádzke infraštruktúry. Komunikácia medzi programovateľnými logickými automatmi (PLC) v ICS predstavuje komplexný tok informácií, ktorý je vystavený rizikám narušenia. Rast objemu týchto dát si vyžaduje pokročilé metódy spracovania, kde tradičné techniky zlyhávajú, a strojové učenie ponúka efektívne riešenie.

Kybernetická bezpečnosť ICS nadobudla na význame po útoku Stuxnet v roku 2010 (Langner 2011), ktorý demonštroval zraniteľnosť PLC voči sofistikovaným kybernetickým hrozbám. Tento incident zdôraznil potrebu moderných bezpečnostných opatrení, ktoré dokážu včas identifikovať a neutralizovať anomálie v dátovej komunikácii. Strojové učenie, so schopnosťou detegovať vzory a odchýlky v dátach, poskytuje revolučný nástroj na ochranu ICS pred útokmi a optimalizáciu ich prevádzky.

Táto práca sa sústreďuje na analýzu komunikácie medzi PLC zariadeniami s využitím strojového učenia na detekciu anomálií. Akékoľvek narušenie komunikácie medzi PLC môže mať vážne dôsledky, preto je kľúčové vybaviť tieto systémy spoľahlivými monitorovacími nástrojmi. Cieľom je navrhnúť a implementovať systém, ktorý efektívne identifikuje anomálie v dátovej komunikácii a zvyšuje bezpečnosť ICS.

Práca sa zaoberá analýzou tradičných metód spracovania dát v ICS a ich obmedzeniami. Predstavuje výber a implementáciu moderných modelov strojového učenia, ako sú 1D CNN, LSTM, iForest a SVM, optimalizovaných na spracovanie časovo korelovaných dát. Výsledkom je komplexná analýza komunikácie ICS, implementácia pokročilých algoritmov na detekciu anomálií

a zhodnotenie ich efektívnosti. Tento prístup prispieva k ochrane kritickej infraštruktúry a k rozvoju technológií nevyhnutných pre moderný priemysel.

Téma práce "Využitie metód strojového učenia pri analýze stochastických signálov pre potreby riadenia procesov" vychádza z pôvodného zadania práce orientovaného na spracovanie astrofyzikálnych signálov. Vzhľadom na vysokoaktuálnu problematiku signálov v inteligentných systémoch riadenia sme sa v tejto práci rozhodli zamerať na kategóriu využitia metód strojového učenia pri analýze digitálnych komunikačných signálov pre potreby riadenia procesov. Digitálne komunikačné signály obsahujú kombináciu deterministických a stochastických vlastností, pričom náhodné faktory ovplyvňujú ich správanie v prenosových kanáloch. Stochastické vlastnosti digitálnych signálov sa prejavujú najmä vo forme náhodného šumu a časových variácií, zatiaľ čo ich štruktúra je deterministická.

Hypotézy dizertačnej práce

Hypotéza 1: Metóda prístupu k monitorovaniu komunikácie PLC v priemyselnej sieti pomocou metód strojového učenia umožní efektívnejšie detegovať potenciálne hrozby, narušenia alebo anomálie v dátovej komunikácii.

Hypotéza 2: Analýza zachytených dátových paketov pri rôznych komunikačných scenároch medzi predkonfigurovanými PLC umožní identifikovať vzorce správania a potenciálne anomálie v komunikácii.

Hypotéza 3: Nezvyčajná komunikácia, charakterizovaná najmä zmenami v inštrukciách alebo pripojením neznámeho zariadenia, indikuje zmenu v komunikačných vzorcoch medzi zariadeniami,

čo môže signalizovať potenciálne narušenie alebo kybernetickú hrozbu v priemyselných riadiacich systémoch.

Ciele dizertačnej práce

1. Analyzovať a zvoliť vhodné nástroje, ktoré umožnia efektívne testovanie a vyhodnotenie zraniteľností a bezpečnostných opatrení v PLC.

2. Vykonať analýzu zachytených dátových paketov medzi predkonfigurovanými PLC v rôznych komunikačných scenároch s cieľom presne identifikovať normálne komunikačné vzorce a vytvoriť dataset pre využitie s nástrojmi AI.

3. Identifikovať potenciálne anomálie v komunikačných paketoch a skúmať ich súvislosť s možnými bezpečnostnými hrozbami alebo narušeniami integrity komunikácie.

4. Aplikovať a porovnať rôzne algoritmy strojového učenia s cieľom navrhnúť optimálny prístup k detekcii bezpečnostných incidentov v reálnom čase.

5. Vyhodnotiť efektívnosť navrhnutého riešenia prostredníctvom analýzy presnosti detekcie hrozieb a anomálií, ako aj jeho schopnosti prispôsobiť sa rôznym scenárom komunikačných narušení.

STU

1 KOMUNIKAČNÉ SIGNÁLY A KYBERNETICKÉ HROZBY V PRIEMYSELNÝCH PROCESOCH

Správny prenos signálov má zásadný význam pre bezpečnosť, spoľahlivosť a efektivitu priemyselných riadiacich systémov. Chyby alebo oneskorenia môžu viesť k nesprávnym rozhodnutiam v riadiacich procesoch, čo môže znížiť kvalitu produkcie, spôsobiť bezpečnostné incidenty alebo poškodenie zariadení. Napríklad nesprávne čítanie teplotného senzora v potravinárskom priemysle môže mať za následok nedostatočnú sterilizáciu, zatiaľ čo v chemickom priemysle môže zlyhanie riadenia tlaku alebo prietoku viesť k haváriám. Na zaistenie kvality signálov sa používajú rôzne opatrenia, ako je kvalitné káblovanie, filtre na minimalizáciu šumu, redundancia a mechanizmy overovania integrity dát pri kritických aplikáciách.

S rastúcou prepojenosťou systémov a nárastom kybernetických hrozieb získava bezpečnosť PLC stále väčšiu prioritu. Tieto systémy riadia kľúčové operácie v priemyselných a kritických infraštruktúrach a ich zraniteľnosti môžu mať vážne následky. Moderné technológie, ako internet, cloudové riešenia a IoT, ktoré sú súčasťou Industry 4.0 a pripravovaného Industry 5.0, umožňujú vyššiu automatizáciu, ale zároveň zvyšujú riziko kybernetických útokov. Tieto útoky môžu zahŕňať malvér, ransomvér alebo sofistikované techniky zamerané na zneužitie zraniteľností v softvéri, protokoloch alebo firmvéri.

Jednou z najväčších hrozieb je nedostatočná autentifikácia, ktorá umožňuje neoprávnený prístup k PLC a manipuláciu s riadiacimi funkciami. Používanie zastaraného hardvéru a softvéru zvyšuje riziko zneužitia známych zraniteľností, pričom nedostatočné šifrovanie komunikácie vystavuje citlivé údaje riziku zachytenia a

manipulácie. Na ochranu pred týmito hrozbami sú kľúčové pravidelné aktualizácie, silná autentifikácia, kontrola prístupu a šifrovanie dát. Monitorovanie sietí a detekcia hrozieb umožňujú včasnú identifikáciu anomálií a ich odstránenie.

Význam pokročilých ochranných opatrení zdôrazňujú aj incidenty, ako je známy útok Stuxnet, ktorý ukázal, že zraniteľnosti ICS môžu byť zneužité na dosiahnutie deštruktívnych cieľov. Moderné PLC systémy, ako napríklad Siemens S7-1500, už integrujú kryptografické mechanizmy na elimináciu zraniteľností, no pretrvávajúce hrozby, ako nedávne zraniteľnosti CVE-2022-1161 či CVE-2022-29833, poukazujú na potrebu ďalšieho zlepšovania bezpečnostných opatrení.

Zabezpečenie ICS vyžaduje kombináciu moderných technológií, zvýšeného povedomia o kybernetickej bezpečnosti a spolupráce medzi vývojármi, bezpečnostnými expertmi a priemyselnými partnermi. Neustále investície a inovácie v tejto oblasti sú nevyhnutné na ochranu kritickej infraštruktúry a zabezpečenie spoľahlivej a efektívnej prevádzky priemyselných procesov. Efektívne opatrenia musia nielen ochraňovať dáta a systémy, ale zároveň posilňovať odolnosť voči narastajúcim kybernetickým hrozbám.

ICS sú moderné technológie využívajúce senzory a algoritmy na zhromažďovanie informácií a optimalizáciu operácií v rôznych oblastiach, ako sú priemyselné procesy, ovládanie budov či doprava. Schopnosť ICS učiť sa z historických údajov a prispôsobovať sa zmenám im umožňuje dynamicky zlepšovať efektivitu, odolnosť a adaptabilitu (Levine 1999). V priemysle tieto systémy maximalizujú výkon pri znižovaní spotreby energie, zatiaľ čo v doprave dokážu v reálnom čase prispôsobiť načasovanie semaforov podľa aktuálnych podmienok, čím zvyšujú plynulosť a bezpečnosť premávky (Hangos a Cameron 2001).

S narastajúcim prepojením ICS na internet rastie význam kybernetickej bezpečnosti. Na ochranu integrity a spoľahlivosti týchto systémov sú nevyhnutné techniky ako šifrovanie, bezpečné komunikačné protokoly a pravidelné bezpečnostné audity. Tieto opatrenia sú kľúčové najmä v citlivých aplikáciách, akými sú priemyselná automatizácia, energetické siete a dopravné systémy.

Správne fungovanie signálov má zásadný význam pre bezpečnosť, spoľahlivosť a efektivitu priemyselných riadiacich systémov. Chyby alebo oneskorenia môžu viesť k nesprávnym rozhodnutiam v riadiacich procesoch, čo môže znížiť kvalitu produkcie, spôsobiť bezpečnostné incidenty alebo poškodenie zariadení. Napríklad nesprávne čítanie teplotného senzora v potravinárskom priemysle môže mať za následok nedostatočnú sterilizáciu, zatiaľ čo v chemickom priemysle môže zlyhanie riadenia tlaku alebo prietoku viesť k haváriám. Na zaistenie kvality signálov sa používajú rôzne opatrenia, ako je kvalitné káblovanie, filtre na minimalizáciu šumu, redundancia a mechanizmy overovania integrity dát pri kritických aplikáciách.

S rastúcou prepojenosťou systémov a nárastom kybernetických hrozieb získava bezpečnosť PLC stále väčšiu prioritu. Tieto systémy riadia kľúčové operácie v priemyselných a kritických infraštruktúrach a ich zraniteľnosti môžu mať vážne následky. Moderné technológie, ako internet, cloudové riešenia a IoT, ktoré sú súčasťou Industry 4.0 a pripravovaného Industry 5.0, umožňujú vyššiu automatizáciu, ale zároveň zvyšujú riziko kybernetických útokov. Tieto útoky môžu zahŕňať malvér, ransomvér alebo sofistikované techniky zamerané na zneužitie zraniteľností v softvéri, protokoloch alebo firmvéri.

Jednou z najväčších hrozieb je nedostatočná autentifikácia, ktorá umožňuje neoprávnený prístup k PLC a manipuláciu s riadiacimi

funkciami. Používanie zastaraného hardvéru a softvéru zvyšuje riziko zneužitia známych zraniteľností, pričom nedostatočné šifrovanie komunikácie vystavuje citlivé údaje riziku zachytenia a manipulácie. Na ochranu pred týmito hrozbami sú kľúčové pravidelné aktualizácie, silná autentifikácia, kontrola prístupu a šifrovanie dát. Monitorovanie sietí a detekcia hrozieb umožňujú včasnú identifikáciu anomálií a ich odstránenie.

Význam pokročilých ochranných opatrení zdôrazňujú aj incidenty, ako je známy útok Stuxnet, ktorý ukázal, že zraniteľnosti ICS môžu byť zneužité na dosiahnutie deštruktívnych cieľov. Moderné PLC systémy, ako napríklad Siemens S7-1500, už integrujú kryptografické mechanizmy na elimináciu zraniteľností, no pretrvávajúce hrozby, ako nedávne zraniteľnosti CVE-2022-1161 či CVE-2022-29833, poukazujú na potrebu ďalšieho zlepšovania bezpečnostných opatrení.

Zabezpečenie ICS vyžaduje kombináciu moderných technológií, zvýšeného povedomia o kybernetickej bezpečnosti a spolupráce medzi vývojármi, bezpečnostnými expertmi a priemyselnými partnermi. Neustále investície a inovácie v tejto oblasti sú nevyhnutné na ochranu kritickej infraštruktúry a zabezpečenie spoľahlivej a efektívnej prevádzky priemyselných procesov. Efektívne opatrenia musia nielen ochraňovať dáta a systémy, ale zároveň posilňovať odolnosť voči narastajúcim kybernetickým hrozbám.

2 STROJOVÉ UČENIE AKO DETEKTOR ANOMÁLNEJ KOMUNIKÁCIE PLC

Návrh algoritmov strojového učenia (ML) zohráva kľúčovú úlohu pri riešení komplexných problémov, akými sú detekcia anomálií a predikcia hrozieb v priemyselných riadiacich systémoch (ICS). V

rámci našej práce sme sa zamerali na vývoj a implementáciu pokročilých algoritmov vrátane 1D CNN, LSTM, iForest a SVM, ktoré sme optimalizovali tak, aby dokázali spracovávať sekvenčné a časovo korelované dáta zozbierané z komunikácie medzi PLC zariadeniami. Naším cieľom bolo zabezpečiť, aby tieto modely spoľahlivo identifikovali odchýlky v normálnom správaní, minimalizovali počet falošných poplachov a boli nasaditeľné v reálnom čase bez kompromisov v ich výkone.

Dáta použité na tréning a testovanie modelov pochádzali z experimentálnych komunikačných scenárov v ICS, pričom dataset bol štruktúrovaný tak, aby zahrnul 60 % normálnych a 40 % anomálnych dát. Normálne dáta reprezentovali typické operácie medzi PLC, ako napríklad prenosy údajov prostredníctvom GET a PUT blokov, ktoré odrážali štandardnú komunikáciu bez narušení. Anomálne dáta boli simulované a zahŕňali rôzne typy kybernetických útokov, medzi ktoré patrili manipulácia s obsahom paketov, injekcia škodlivých príkazov a útoky typu preťaženia siete (flooding). Celkový dataset obsahoval 10 000 vzoriek, ktoré boli rozdelené do tréningovej, validačnej a testovacej množiny v pomere 70:15:15. Každá vzorka obsahovala kľúčové parametre komunikácie, ako sú časové pečiatky, zdrojové a cieľové IP adresy, čísla portov a obsah payloadu, čo umožnilo modelom strojového učenia presne analyzovať a detegovať vzory v dátach.

Pri návrhu architektúry modelov sme uplatnili iteratívny prístup s dôrazom na experimentovanie a optimalizáciu. Pre 1D CNN sme starostlivo ladili parametre, ako sú počet a veľkosť konvolučných filtrov, krok (stride) a počet pooling vrstiev. Tieto nastavenia boli optimalizované tak, aby umožňovali extrakciu komplexných čŕt z dát, ktoré sú typické pre ICS komunikáciu. Architektúra LSTM bola navrhnutá na efektívne spracovanie časových závislostí medzi dátovými vzorkami, pričom sme aplikovali techniky, ako je dropout, na minimalizáciu rizika pretrénovania modelu. Pre SVM

sme testovali rôzne kernelové funkcie, ako lineárne a radiálne bázové funkcie (RBF), a upravovali sme penalizačné parametre (C), aby sme našli optimálnu rovnováhu medzi generalizáciou a presnosťou. Model iForest bol konfigurovaný s ohľadom na parametre, ako je počet stromov a maximálna hĺbka, aby dokázal efektívne identifikovať odľahlé hodnoty reprezentujúce anomálie.

Výkon modelov sme hodnotili pomocou metrík, ako sú presnosť, F1 skóre, precision a recall, ktoré poskytujú komplexný pohľad na schopnosť modelov správne klasifikovať normálne a anomálne dáta. Použitie confusion matrix nám umožnilo analyzovať detaily predikcií a zamerať sa na minimalizáciu falošných poplachov. Okrem presnosti sme monitorovali aj výpočtový čas modelov, čím sme zabezpečili ich vhodnosť na nasadenie v reálnych časových podmienkach. Napríklad 1D CNN dosiahla najvyššiu presnosť 92 % s F1 skóre 0,91, zatiaľ čo jej výpočtový čas bol menej ako 0,8 sekundy na vzorku, čo potvrdzuje jej použiteľnosť v scenároch vyžadujúcich rýchlu detekciu.

Iteratívny proces návrhu zahŕňal dôslednú verifikáciu modelov, aby sme zabezpečili, že implementácia je v súlade so špecifikáciami a že modely spoľahlivo reagujú na reálne scenáre ICS komunikácie. Validácia na nevidených dátach ukázala schopnosť modelov generalizovať na nové typy narušení, čo potvrdilo ich robustnosť. Tento proces umožnil vytvoriť modely, ktoré sú nielen presné, ale aj odolné voči dynamickým výzvam spojeným s bezpečnosťou ICS.

Náš prístup predstavuje významný pokrok v oblasti kybernetickej bezpečnosti priemyselných systémov. Kombinácia reálnych dát, pokročilých algoritmov a optimalizovaných architektúr nám umožnila vytvoriť systém, ktorý je schopný efektívne detegovať široké spektrum anomálií a minimalizovať riziká spojené s kybernetickými útokmi. Táto práca nielenže prispieva k ochrane

kritickej infraštruktúry, ale poskytuje aj pevný základ pre ďalší výskum a vývoj sofistikovaných riešení v oblasti strojového učenia a kybernetickej bezpečnosti ICS.

3 ZHRNUTIE VÝSLEDKOV VYKONANEJ ANALÝZY

V oblasti detekcie anomálií v priemyselných riadiacich systémoch (ICS) boli tradičné metódy založené na pravidlách a signatúrach dlhodobo štandardným prístupom, ktorý dominoval v kybernetickej bezpečnosti. Tieto techniky využívali vopred definované vzory útokov alebo odchýlky od normálneho správania na identifikáciu bezpečnostných incidentov. Ich hlavnou výhodou bola presnosť pri dobre definovaných hrozbách, nízka miera falošne pozitívnych poplachov a jednoduchosť implementácie v prostrediach s relatívne stabilnou prevádzkou. Tieto faktory prispeli k ich popularite, najmä v systémoch, kde bola kontinuita prevádzky kritická. Napriek týmto benefitom mali tieto metódy výrazné obmedzenia, predovšetkým ich neschopnosť detegovať nové, neznáme hrozby alebo adaptovať sa na dynamicky sa meniace prostredia ICS. Útočníci, využívajúc tieto medzery, mohli ľahko vyvinúť sofistikované techniky obchádzajúce pravidlá a signatúry, čo významne znížilo účinnosť týchto systémov.

V reakcii na tieto výzvy sme implementovali pokročilé algoritmy strojového učenia, ktoré predstavujú zásadný pokrok v oblasti detekcie anomálií. Modely ako 1D CNN, LSTM, iForest a SVM prinášajú schopnosť autonómne analyzovať rozsiahle datasety, modelovať normálne správanie systému a detegovať odchýlky naznačujúce potenciálne útoky. Na rozdiel od tradičných metód tieto modely dokážu detegovať nielen známe hrozby, ale aj nepredvídané vzory správania, ktoré nie sú explicitne definované v pravidlách. To ich robí obzvlášť účinnými v moderných ICS, kde

hrozby neustále evolvujú a nové útoky vznikajú s rastúcou komplexnosťou.

Naše modely prinášajú revolučnú schopnosť adaptovať sa na dynamické podmienky ICS. Zatiaľ čo pravidlovo založené systémy si vyžadujú manuálnu aktualizáciu databáz signatúr a pravidiel, modely strojového učenia sa dokážu priebežne učiť z nových dát a zlepšovať svoje predikčné schopnosti autonómne. Tento proces výrazne znižuje potrebu manuálnych zásahov, čím sa zvyšuje efektivita a rýchlosť detekcie hrozieb. Aj keď implementácia týchto modelov vyžaduje rozsiahle datasety na trénovanie a vysoké výpočtové zdroje, ich schopnosť spracovávať veľké objemy dát a identifikovať široké spektrum hrozieb ich robí ideálnymi pre moderné aplikácie.

V porovnaní s tradičnými technikami strojového učenia, ako sú SVM, kNN alebo rozhodovacie stromy, ktoré sa v minulosti často používali, sme v našej práci využili pokročilé algoritmy špecificky navrhnuté na spracovanie sekvenčných dát typických pre ICS komunikáciu. Napríklad model 1D CNN, navrhnutý na extrakciu komplexných čŕt z dát, dosiahol vysokú presnosť pri detekcii manipulácie s payloadom alebo neautorizovaných zmien konfigurácií. LSTM, na druhej strane, preukázal výnimočné schopnosti pri identifikácii časových závislostí a zachytávaní dynamických procesov, čím bol ideálny pre analýzu zložitejších scenárov. Naša práca zároveň ukázala, že hodnotenie modelov na základe metrík ako F1 skóre, precision a recall je nevyhnutné pre optimalizáciu výkonnosti a minimalizáciu falošne pozitívnych a negatívnych klasifikácií.

Jedným z kľúčových aspektov našej práce bola práca s dátami zachytenými priamo z reálnej komunikácie ICS. Na rozdiel od predchádzajúcich štúdií, ktoré sa spoliehali na statické datasety, ako KDD Cup alebo NSL-KDD, naše dáta pochádzali z reálnych

experimentálnych nastavení. Tento dynamický dataset lepšie odrážal reálne výzvy a potreby moderných priemyselných systémov, ako sú vysoké požiadavky na spoľahlivosť a presnosť. Práca s reálnymi dátami umožnila vytvoriť modely, ktoré sú nielen presné, ale aj schopné zvládať praktické scenáre v ICS.

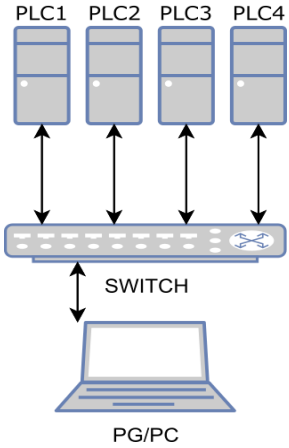
Adaptabilita a škálovateľnosť našich modelov predstavujú ďalší významný prínos. Naše riešenia sú schopné generalizovať na široké spektrum narušení a scenárov, čo ich robí robustnými voči dynamickým zmenám v prostredí ICS. Modely, ako 1D CNN a LSTM, navyše preukázali schopnosť identifikovať subtílne zmeny v komunikácii, ktoré tradičné metódy mohli prehliadnuť. Táto schopnosť je zásadná pre ochranu kritickej infraštruktúry, kde aj drobné odchýlky môžu mať vážne dôsledky.

Naše výsledky preukázali, že pokročilé metódy strojového učenia významne prekonávajú tradičné prístupy v oblasti detekcie anomálií. Tieto metódy nielen zvyšujú presnosť detekcie, ale umožňujú aj flexibilitu a adaptáciu na meniace sa podmienky a nové hrozby. Týmto spôsobom prispievajú k ochrane priemyselných systémov pred rastúcimi kybernetickými hrozbami. Tento pokrok predstavuje pevný základ pre ďalší vývoj sofistikovaných bezpečnostných systémov v priemyselných riadiacich systémoch, čím sa zvyšuje bezpečnosť a odolnosť kritickej infraštruktúry voči stále sofistikovanejším útokom. Veríme, že naše výsledky budú slúžiť ako inšpirácia pre ďalší výskum a vývoj riešení na ochranu ICS po celom svete.

4 NÁVRH HARDVÉROVÉHO VYHOTOVENIA ZAPOJENIA

V našom prípade sme v laboratórnych podmienkach zachytávali komunikáciu štyroch PLC, pričom sme mali pripojený počítač, na

ktorom sme ich komunikáciu zachytávali. Na účely zberu dát sme navrhli systém, ktorý je hardvérovo neutrálny, čo znamená, že nie je obmedzený len na použitie so zariadeniami PLC od spoločnosti Siemens; je kompatibilný aj s PLC od iných výrobcov.



Obr. 1: Architektúra zapojenia PLC pre zachytenie ich komunikácie

V rámci experimentálneho nastavenia sme použili 4 nezávislé PLC S7-300, ktoré sme prepojili prostredníctvom 5-portového prepínača NETGEAR GS305E. Výber PLC typu S7-300 bol motivovaný praktickými dôvodmi: tento typ PLC je široko používaný v priemyselných aplikáciách v reálnom svete a z kybernetického hľadiska neobsahuje špecifické bezpečnostné prvky.

Tab. 1: Technické parametre použitých PLC S7-300

Pamäťová kapacita PLC	**64 kB (závisí od konkrétneho modelu S7-300)**
CPU typ	CPU 315-2 DP

Pracovná frekvencia CPU	1 MHz
Komunikačný protokol	Profinet, Industrial Ethernet
Rýchlosť prenosu dát	100 Mbps
Napájacie napätie PLC	24 V DC
Počet vstupov/výstupov	16 digitálnych vstupov, 16 digitálnych výstupov
Sieťové prepojenie	5-portový prepínač NETGEAR GS305E
Maximálna dĺžka kábla	100 m (Ethernet štandard)
Zbernicové rozhranie	MPI (Multi-Point Interface), Profibus
Prostredie	Laboratórne podmienky
Operačná teplota	0 °C až +60 °C
Krytie (IP)	IP20
Softvérový nástroj	TIA Portal (Siemens), kompatibilný aj s inými konfigurátormi
Čas cyklu CPU	~2 ms pre malý program (závisí od zložitosti programu)

5 NÁVRH SOFTVÉROVÉHO RIEŠENIA

Táto práca sa zameriava na vývoj robustného systému schopného detegovať anomálie a minimalizovať kybernetické hrozby v ICS. Pre tento účel sme vytvorili detailne analyzovaný dataset zachytávajúci normálnu aj anomálnu komunikáciu medzi PLC zariadeniami, pričom sme aplikovali sofistikované algoritmy na čistenie dát a prípravu datasetu.

Pri návrhu logiky bol kladený dôraz na simuláciu realistických prevádzkových aj anomálnych scenárov komunikácie. Testovacie slučky overovali správnosť implementácie simulovaných útokov, ako aj presnosť vykonávania základných funkcií programu.

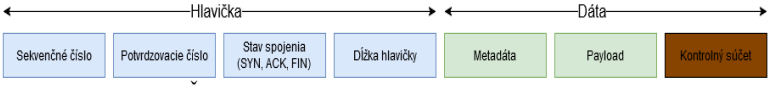
Simulované útoky zahŕňali manipulácie s dátami, injekciu škodlivých príkazov a preťaženie komunikácie. Tento prístup minimalizoval riziko chýb a poskytoval spoľahlivé dáta pre tréning modelov strojového učenia.

Zachytené dáta zo simulácií boli spracovávané pomocou špeciálne navrhnutých algoritmov na analýzu pravdepodobnostných vzťahov medzi jednotlivými komponentmi komunikácie. Tieto algoritmy boli schopné identifikovať prirodzené odchýlky v dátach, ako sú časové fluktuácie alebo nepravidelnosti v synchronizácii príkazov GET/PUT. Pri modelovaní normálnej komunikácie sme implementovali stochastické parametre, ktoré predikovali očakávané hodnoty pre polia paketov, ako sú IP adresy, veľkosť dát a obsah payloadu. Akékoľvek výrazné odchýlky, ako náhle zmeny v časovaní alebo neštandardné hodnoty payloadu, boli okamžite označené na ďalšiu analýzu.

Tento prístup umožnil detekciu anomálií s vysokou presnosťou, pričom minimalizoval falošne negatívne výsledky a zabezpečil spoľahlivosť systému aj v dynamických podmienkach. Využitím stochastických metód sme zvýšili adaptabilitu systému na neočakávané zmeny v komunikácii, čím sme zlepšili jeho schopnosť identifikovať potenciálne hrozby. Táto schopnosť je kľúčová v priemyselných riadiacich systémoch, kde aj drobné nezrovnalosti môžu mať závažné dôsledky na bezpečnosť a efektivitu prevádzky. Kombinácia stochastických parametrov, robustných algoritmov a realistických simulácií poskytuje základ pre spoľahlivé a presné riešenia v oblasti kybernetickej bezpečnosti ICS.

Pri analýze komunikačných paketov sme zaznamenali stochastické správanie, ktoré zahŕňalo prirodzené variácie v časových radoch spôsobené preťažením siete, kolísaním prenosovej rýchlosti alebo nesynchronizáciou príkazov GET a PUT medzi zariadeniami.

Tieto odchýlky sme zahrnuli do prediktívnych modelov strojového učenia, čo umožnilo systému odlíšiť normálne správanie od potenciálnych hrozieb. Zachytené pakety obsahovali kľúčové informácie, ako sú IP adresy, porty, časové pečiatky a payload, ktoré sme použili na identifikáciu odchýlok naznačujúcich kybernetické útoky.



Obr. 2: Štruktúra zachytávaných komunikačných paketov

Dataset sme tvorili kombináciou reálnych a simulovaných údajov. Počas normálnej prevádzky sme zachytili 3000 vzoriek obsahujúcich štandardné operácie medzi PLC, ako sú príkazy GET a PUT, ktoré slúžili ako referenčný základ pre tréning modelov. Na druhej strane anomálne dáta vznikli simuláciou realistických kybernetických útokov, ako sú replay útoky, manipulácie s payloadom a flooding útoky. Tieto útoky sme integrovali do komunikácie s cieľom otestovať schopnosti detekcie algoritmov. Anomálnych paketov bolo zachytených 2000. Následne bolo ešte simulovaných 3000 normálnych komunikačných paketov a 2000 anomálnych.

Proces čistenia dát zahŕňal odstránenie nesúvisiacich, poškodených a redundantných záznamov. Boli aplikované techniky na normalizáciu časových značiek a validáciu integrity paketov, čo zabezpečilo ich konzistenciu a presnosť. Redundancia bola eliminovaná s cieľom zvýšiť unikátnosť záznamov a minimalizovať riziko skreslenia modelov. Payload bol analyzovaný na úrovni štruktúry, aby sa overila jeho správnosť a formátovanie.

Výsledný dataset obsahoval 6000 normálnych a 4000 anomálnych vzoriek rozdelených na tréningovú, validačnú a testovaciu

množinu. Vysoká kvalita dát umožnila presné trénovanie modelov strojového učenia, čo zvýšilo spoľahlivosť a efektívnosť detekcie anomálií v ICS. Tento prístup vytvára pevný základ pre vývoj a nasadenie robustných systémov na ochranu kritickej infraštruktúry pred modernými kybernetickými hrozbami.

6 VYHODNOTENIE VÝSLEDKOV A PRÍNOS PRÁCE

Výsledky testovania algoritmov LSTM, iForest, 1D CNN a SVM odhalili zásadné rozdiely vo výkonnosti, pričom každý model má svoje špecifické výhody a nevýhody v kontexte detekcie anomálií v komunikácii PLC v ICS.

LSTM vykazuje schopnosť zachytiť časové závislosti v dátach, s presnosťou trénovania 89 % a testovania 75 %, a F1 skóre 0,77 naznačuje vyvážený výkon medzi precision a recall. Model bol účinný pri detekcii postupne sa vyvíjajúcich útokov, no jeho spracovanie trvá 2,5 sekundy, čo obmedzuje jeho využitie v reálnom čase a pri náhlych odchýlkach.

iForest dosiahol presnosť testovania 70 % a F1 skóre 0,68, čo ukazuje na jeho efektívnosť pri základných analýzach dát. S jednoduchou implementáciou a nízkymi požiadavkami na označovanie dát sa hodí na rýchle predbežné analýzy. Nevýhodou je jeho nižšia presnosť a neschopnosť identifikovať komplexné anomálie, pričom čas spracovania je 3 sekundy.
1D CNN preukázala najvyšší výkon, s presnosťou trénovania 91 %, testovaním 92 % a F1 skóre 0,91. Model exceluje pri detekcii jemných odchýlok, ako sú manipulácie s payloadom, pričom jeho predikcia trvá iba 0,79 sekundy. Výpočtová náročnosť počas tréningu je jeho slabinou, ale jeho výhody v presnosti a rýchlosti ho robia ideálnym pre aplikácie v reálnom čase.

SVM dosiahlo najnižšiu presnosť (51 % pre tréning a 52 % pre testovanie) a F1 skóre 0,51, pričom trpí vysokou mierou falošne pozitívnych klasifikácií. Napriek svojej jednoduchosti sa SVM ukázalo ako nevhodné pre komplexné a vysokodimenzionálne dáta ICS.

Záverom je, že 1D CNN je najlepším riešením pre detekciu anomálií v ICS, pričom kombinuje presnosť, rýchlosť a schopnosť spracovávať komplexné dáta. LSTM je vhodné na analýzu časových závislostí, zatiaľ čo iForest je efektívny nástroj na predbežné analýzy. Naopak, SVM má výrazné obmedzenia, ktoré ho robia nevhodným pre dynamické prostredia ICS.

Tab. 2: Celkové porovnanie použitých ML algoritmov

ML Algoritmus	LSTM	iForest	1D CNN	SVM
Trénovacia presnosť	0,89	0,72	0,91	0,51
Testovacia presnosť	0,75	0,70	0,92	0,52
F1 skóre	0,77	0,68	0,91	0,51
Pravdivo pozitívne	18,75	17,5	23	13
Nepravdivo pozitívne	18,75	22,5	5,9	36
Pravdivo negatívne	56,25	52,5	69	39
Nepravdivo negatívne	6,25	7,5	1,9	12
Precision	0,5	0,44	0,79	0,27
Recall	0,75	0,7	0,92	0,52

Výpočtový čas predikcie [s]	2,5	3	0,79	4,8

Významný prínos tejto práce spočíva v preukázaní, že moderné metódy strojového učenia sú nielen vhodné, ale aj vysoko účinné na detekciu anomálií v ICS. Naše výsledky jasne ukázali, že algoritmy strojového učenia dokážu spoľahlivo identifikovať aj subtílne zmeny v komunikačných vzorcoch, ktoré by mohli byť pre tradičné metódy nerozpoznateľné. Tieto zmeny často naznačujú začiatok potenciálnych kybernetických hrozieb, ktoré by mohli ohroziť bezpečnosť a stabilitu kritickej infraštruktúry. Naše experimenty preukázali, že metódy ako 1D CNN a LSTM dokážu efektívne extrahovať a analyzovať časové a priestorové črty v dátach, čo zvyšuje presnosť detekcie hrozieb v reálnom čase.

Okrem schopnosti detegovať subtílne zmeny sme preukázali aj širokú flexibilitu navrhnutých modelov, ktorá umožňuje ich adaptáciu na rôzne typy narušení. Táto flexibilita je zásadná pre dynamické prostredie ICS, kde sa hrozby neustále menia a vyvíjajú. Modely dokázali identifikovať rôzne druhy útokov, od manipulácie s údajmi až po komplexné scénáre, ako sú replay útoky, man-in-the-middle a preťaženie siete (flooding). Schopnosť našich modelov prispôsobiť sa takýmto rôznorodým scenárom výrazne zvyšuje ich praktickú využiteľnosť, najmä v prostrediach, kde je kľúčové identifikovať anomálie v reálnom čase s minimálnym počtom falošne pozitívnych a falošne negatívnych výsledkov.

Navyše sme demonštrovali, že moderné metódy strojového učenia dokážu prekonať tradičné pravidlové a signatúrne prístupy, ktoré sú obmedzené svojou neschopnosťou reagovať na neznáme alebo nové hrozby. Tento pokrok je obzvlášť dôležitý v kontexte rastúcich kybernetických hrozieb, ktoré čoraz častejšie cielia na

kritickú infraštruktúru a priemyselné systémy. Naše riešenie navyše dokazuje, že metódy strojového učenia dokážu nielen identifikovať hrozby, ale zároveň poskytujú operátorom cenné informácie o charaktere a pôvode anomálií, čo môže výrazne uľahčiť ich riešenie a minimalizovať potenciálne škody.

Praktická nasaditeľnosť navrhnutých modelov v reálnom čase bola zabezpečená optimalizáciou ich výpočtovej náročnosti a výkonnosti. To umožňuje ich implementáciu aj v prostrediach s obmedzenými zdrojmi, kde je čas kritickým faktorom. Táto schopnosť spracovávať veľké objemy dát v krátkom čase robí naše riešenie atraktívnym pre široké spektrum priemyselných aplikácií.

Táto práca teda nielenže prispieva k rozvoju modernej kybernetickej bezpečnosti, ale zároveň otvára nové možnosti pre integráciu pokročilých algoritmov strojového učenia do existujúcich monitorovacích a ochranných systémov ICS. Veríme, že naše výsledky môžu slúžiť ako pevný základ pre ďalší výskum a vývoj robustných bezpečnostných mechanizmov, ktoré dokážu čeliť narastajúcej komplexnosti a sofistikovanosti kybernetických hrozieb v priemyselných riadiacich systémoch.
Budúci výskum chceme zamerať na integráciu navrhnutých algoritmov strojového učenia do širších rámcov ochrany kybernetickej bezpečnosti ICS. Táto integrácia zahŕňala nielen detekciu anomálií, ale aj vývoj systémov, ktoré dokážu automaticky reagovať na identifikované hrozby. Aktívne opatrenia, ako izolácia podozrivých zariadení, dynamická rekonfigurácia siete alebo zablokovanie narušených komunikácií, sú nevyhnutné na minimalizáciu škôd spôsobených kybernetickými útokmi.

Jedným z hlavných cieľov budúceho výskumu je vývoj hybridných modelov, ktoré kombinujú silné stránky viacerých algoritmov strojového učenia. Napríklad kombinácia 1D CNN na extrakciu

priestorových čŕt z dát s LSTM na analýzu časových vzorcov môže výrazne zvýšiť presnosť a robustnosť detekcie. Tieto hybridné modely by mohli byť schopné spracovávať komplexné vzory narušenia, ktoré sú často distribuované cez čas a priestor v rámci siete ICS.

Ďalšou dôležitou oblasťou výskumu je federatívne učenie, ktoré umožňuje trénovanie modelov na decentralizovaných dátach bez potreby ich prenosu na centrálny server. Tento prístup je obzvlášť užitočný v ICS, kde môže byť zdieľanie citlivých dát medzi zariadeniami alebo organizáciami obmedzené z dôvodu bezpečnosti alebo ochrany súkromia. Federatívne modely dokážu zachovať lokálne dáta na jednotlivých uzloch, pričom centrálne spracovanie zahŕňa iba agregáciu aktualizácií modelov. Tento prístup znižuje riziko úniku údajov a umožňuje škálovanie ochranných opatrení na širšiu sieť ICS.

Okrem technických aspektov je nevyhnutné zaoberať sa aj legislatívnymi a etickými otázkami spojenými so zavádzaním systémov strojového učenia do kritickej infraštruktúry. Potreba transparentnosti a vysvetliteľnosti algoritmov, známa ako Explainable AI (XAI), je kľúčová na získanie dôvery užívateľov a prevádzkovateľov ICS. XAI poskytuje jasné vysvetlenia, prečo model označil konkrétne správanie ako anomálne, čo uľahčuje identifikáciu falošne pozitívnych výsledkov a zvyšuje akceptáciu týchto systémov.

Rozšírenie datasetov o nové typy anomálií a scenárov útokov je ďalším kľúčovým krokom na zvýšenie robustnosti modelov. Zahrnutie dát z rôznych priemyselných odvetví a geografických lokalít by mohlo výrazne zlepšiť schopnosť modelov generalizovať a prispôsobiť sa rôznym prostrediam. Navyše, rozvoj techník syntetického obohacovania datasetov, ako generatívne

adversariálne siete (GAN), môže pomôcť prekonať problémy s nedostatkom reálnych dát, čo je častým problémom v oblasti ICS. Dôležitou výzvou zostáva optimalizácia výpočtovej náročnosti modelov, aby boli schopné fungovať v reálnom čase na obmedzených hardvérových zdrojoch bežných v priemyselných prostrediach. Implementácia ľahkých modelov alebo využitie akcelerátorov, ako sú GPU a TPU, môže výrazne skrátiť čas spracovania a zlepšiť praktickú nasaditeľnosť riešení.

Napokon, významným smerom výskumu je vývoj integrovaných systémov kybernetickej bezpečnosti, ktoré dokážu kombinovať detekciu anomálií s ďalšími ochranami, ako sú prevencia útokov, monitorovanie siete a systémové zálohovanie. Tieto systémy by mali byť navrhnuté tak, aby fungovali ako jednotná platforma schopná nielen detegovať a reagovať na hrozby, ale aj poskytovať analytické nástroje na predikciu budúcich útokov.

Táto práca predstavuje významný krok k budovaniu bezpečnejšej a odolnejšej infraštruktúry ICS. Naše výsledky ukázali, že moderné technológie strojového učenia dokážu poskytnúť efektívne riešenia na detekciu anomálií a ochranu priemyselných systémov. Veríme, že táto práca nielenže podporí ďalší výskum v oblasti kybernetickej bezpečnosti, ale aj pomôže pri vývoji praktických a škálovateľných riešení pre ochranu kritickej infraštruktúry po celom svete.

ZÁVER

Cieľom tejto práce bolo navrhnúť a implementovať systém na detekciu anomálií v komunikácii ICS s využitím strojového učenia. Zamerali sme sa na spoľahlivé riešenie schopné presne identifikovať narušenia a potenciálne kybernetické hrozby v dátovej komunikácii medzi PLC. Práca zahŕňala celý proces od tvorby datasetu cez návrh a optimalizáciu modelov až po ich

testovanie a validáciu, čím sme overili ich vhodnosť pre túto špecifickú oblasť.

Jadro práce tvoril návrh datasetu založeného na sniffingu komunikácie medzi PLC. Dáta reprezentovali reálne scenáre, vrátane štandardnej komunikácie a simulovaných kybernetických útokov. Dataset obsahoval 6000 normálnych a 4000 anomálnych vzoriek, pričom kvalita a štruktúra dát zabezpečili robustný základ pre tréning modelov. Anomálie boli simulované zmenami v payloadoch, hlavičkách paketov a narušením časových vzorcov, čo umožnilo realistickú prípravu dát pre identifikáciu rôznych typov narušení.

Modely strojového učenia, vrátane 1D CNN, LSTM, SVM a iForest, boli optimalizované a testované na tomto datasete. Z analýzy výsledkov vyplýva, že 1D CNN dosiahla najlepšiu výkonnosť s presnosťou 92 % a F1 skóre 0,91, čo ukazuje na jej schopnosť presne klasifikovať dáta a minimalizovať falošné detekcie. LSTM preukázalo výnimočné schopnosti pri zachytávaní časových vzťahov, zatiaľ čo iForest bol efektívny pri analýzach, kde neboli dostupné rozsiahle anotované dáta. Naproti tomu SVM vykázalo nižšiu presnosť, čo naznačuje jeho obmedzenia pri zložitých a vysokodimenzionálnych dátach.

Výsledky práce preukázali, že moderné metódy strojového učenia dokážu efektívne detegovať aj subtílne zmeny v komunikácii, ktoré môžu naznačovať kybernetické hrozby. Flexibilita týchto modelov umožňuje ich adaptáciu na rôzne narušenia, čo zvyšuje ich praktickú využiteľnosť. Práca má širší význam pre oblasť kybernetickej bezpečnosti kritickej infraštruktúry, kde narastajúce hrozby vyžadujú inovatívne riešenia na monitorovanie a detekciu útokov.

Do budúcnosti plánujeme rozšíriť dataset o ďalšie scenáre narušení a integrovať modely do reálnych systémov ICS na overenie ich výkonnosti v praxi. Taktiež vidíme potenciál v kombinácii s hybridnými modelmi a federatívnym učením, ktoré môžu zlepšiť ochranu decentralizovaných systémov. Táto práca poskytuje základ pre ďalší výskum a vývoj robustných mechanizmov na zvýšenie bezpečnosti a spoľahlivosti priemyselných riadiacich systémov, čím prispieva k ochrane kritickej infraštruktúry pred modernými kybernetickými hrozbami.

VÝBER Z BIBLIOGRAFICKÝCH ODKAZOV

ABDULREZZAK, Sarah a Firas SABIR, 2023. An Empirical Investigation on Snort NIDS versus Supervised Machine Learning Classifiers. *Journal of Engineering* [online]. 2023, roč. 29, č. 2, s. 164–178 [cit. 16.3.2024]. ISSN 2520-3339, 1726-4073. Dostupné na: doi:10.31026/j.eng.2023.02.11

ABOAH BOATENG, Emmanuel a J. W. BRUCE, 2022. Unsupervised Machine Learning Techniques for Detecting PLC Process Control Anomalies. *Journal of Cybersecurity and Privacy* [online]. 2022, roč. 2, č. 2, s. 220–244 [cit. 16.3.2024]. ISSN 2624-800X. Dostupné na: doi:10.3390/jcp2020012

ALPAYDIN, Ethem, 2020. Introduction to machine learning. Fourth edition. Cambridge, Massachusetts London: The MIT Press. Adaptive computation and machine learning. ISBN 978-0-262-04379-3.

ALTUNAY, Hakan Can a Zafer ALBAYRAK, 2023. A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks. Engineering Science and Technology, an International Journal [online]. 2023, roč. 38, s. 101322 [cit. 16.3.2024]. ISSN 22150986. Dostupné na: doi:10.1016/j.jestch.2022.101322

ANDERSON, T. W. a D. A. DARLING, 1952. Asymptotic Theory of Certain "Goodness of Fit" Criteria Based on Stochastic Processes. The Annals of Mathematical Statistics [online]. 1952, roč. 23, č. 2, s. 193–212 [cit. 8.12.2024]. ISSN 0003-4851. Dostupné na: doi:10.1214/aoms/1177729437

HANGOS, K. M. a Ian CAMERON, 2001. *Process modelling and model analysis*. San Diego: Academic Press. Process systems engineering, v. 4. ISBN 978-0-12-156931-0.

LANGNER, Ralph, 2011. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy Magazine* [online]. 2011, roč. 9, č. 3, s. 49–51 [cit. 16.3.2024]. ISSN 1540-7993. Dostupné na: doi:10.1109/MSP.2011.67

LEVINE, Ross, 1999. *Bank-Based and Market-Based Financial Systems: Cross-Country Comparisons* [online]. B.m.: The World Bank. Policy Research Working Papers [cit. 8.12.2024]. Dostupné na: doi:10.1596/1813-9450-2143

MCGILL, Tanya a Nik THOMPSON, 2017. Old risks, new challenges: exploring differences in security between home computer and mobile device use. *Behaviour & Information Technology* [online]. 2017, roč. 36, č. 11, s. 1111–1124 [cit. 8.12.2024]. ISSN 0144-929X, 1362-3001. Dostupné na: doi:10.1080/0144929X.2017.1352028

MENDELSOHN, K. J., 2000. *Trend Forecasting With Technical Analysis*. Ellicott City (Maryland): Marketplace Books. Trade Secrets Series.

MUKHOPADHYAY, Nitis, 2000. *Probability and Statistical Inference*. Milton: Taylor & Francis Group. Statistics: a Series of Textbooks and Monographs. ISBN 978-0-8247-0379-0.

PRIESTLEY, Maurice B. a M. B. PRIESTLEY, 2004. *Spectral analysis and time series*. Repr. Amsterdam Heidelberg: Elsevier. Probability and mathematical statistics. ISBN 978-0-12-564922-3.

PROAKIS, John G. a Dimitris G. MANOLAKIS, 1996. *Digital signal processing: principles, algorithms, and applications*. 3. ed. Upper Saddle River: Prentice Hall. ISBN 978-0-13-373762-2.

ZOZNAM PUBLIKAČNEJ ČINNOSTI

V2 Vedecký výstup publikačnej činnosti ako časť editovanej knihy alebo zborníka

V2_01 BENKA, Denis - VAŠOVÁ, Sabína - KEBÍSEK, Michal - STRÉMY, Maximilián. Detection of Variable Astrophysical Signal Using Selected Machine Learning Methods. In *Artificial Intelligence Application in Networks and Systems : Proceedings of 12th Computer Science On-line Conference 2023, Volume 3*. 1. vyd. Cham : Springer Nature, 2023, S. 679-691. ISSN 2367-3370. ISBN 978-3-031-35313-0 (2023: 0.171 - SJR, Q4 - SJR Best Q). V databáze: DOI: 10.1007/978-3-031-35314-7_57 ; SCOPUS: 2-s2.0-85172738170. Typ výstupu: príspevok z podujatia; Výstup: zahraničný; Kategória publikácie do 2021: AFC

V2_02 BENKA, Denis - DOBROTKA, Andrej - STRÉMY, Maximilián. Detection of Quasi-Periodic Oscillations in Time Series of a Cataclysmic Variable Using Support Vector Machine. In *Machine Learning for Astrophysics*

: proceedings of the ML4Astro International Conference, 30 May - 1 Jun 2022, Catania, Sicilia. 1. vyd. Cham : Springer, 2023, S. 11-13. ISSN 1570-6591. ISBN 978-3-031-34166-3 (print). V databáze: DOI: 10.1007/978-3-031-34167-0_3 ; SCOPUS: 2-s2.0-85175957891.
Typ výstupu: príspevok z podujatia; Výstup: zahraničný; Kategória publikácie do 2021: AFC

V2_03 BENKA, Denis - GAŠPAR, Gabriel - NEMLAHOVÁ, Veronika - NEMLAHA, Eduard - BUDJAČ, Roman. Proposal of a Remote-Control System for Building Lighting Managemenet. In *21st Mechatronika 2024 : Proceedings of the 21st International Conference on Mechatronics - Mechatronika (ME), 4-6 December 2024, Brno, Czech Republic*. 1. vyd. Praha : Czech Technical University in Prague, 2024, S. 109-113. ISBN 979-8-3503-9489-4 (USB).
Typ výstupu: príspevok z podujatia; Výstup: zahraničný; Kategória publikácie do 2021: AFC

V2_04 BENKA, Denis - GAŠPAR, Gabriel - BUDJAČ, Roman - ELIÁŠ, Rastislav - SKOVAJSA, Martin. Design and Implementation of the Grouting Process Measurement Device with a Datalogger. In *21st Mechatronika 2024 : Proceedings of the 21st International Conference on Mechatronics - Mechatronika (ME), 4-6 December 2024, Brno, Czech Republic*. 1. vyd. Praha : Czech Technical University in Prague, 2024, S. 247-260. ISBN 979-8-3503-9489-4 (USB).
Typ výstupu: príspevok z podujatia; Výstup: zahraničný; Kategória publikácie do 2021: AFC

STU

V2_05 VAŠOVÁ, Sabína - BENKA, Denis - DOBROTKA, Andrej - STRÉMY, Maximilián. The feasibility of a convolutional neural network in the detection of variable phenomena in astronomical observations. In *International Doctoral Seminar 2022 : 27. - 28. 04. 2022, Smolenice, SR*. 1. vyd. Trnava : AlumniPress, 2022, S. 323-337. ISBN 978-80-8096-292-0.
Typ výstupu: príspevok z podujatia; Výstup: domáci; Kategória publikácie do 2021: AFD

V2_06 VAŠOVÁ, Sabína - BENKA, Denis - KEBÍSEK, Michal - STRÉMY, Maximilián. Land Cover Detection in Slovak Republic Using Machine Learning. In *Artificial Intelligence Application in Networks and Systems : Proceedings of 12th Computer Science Online Conference 2023, Volume 3*. 1. vyd. Cham : Springer Nature, 2023, S. 692-702. ISSN 2367-3370. ISBN 978-3-031-35313-0 (2023: 0.171 - SJR, Q4 - SJR Best Q). V databáze: DOI: 10.1007/978-3-031-35314-7_58 ; SCOPUS: 2-s2.0-85172736070.
Typ výstupu: príspevok z podujatia; Výstup: zahraničný; Kategória publikácie do 2021: AFC

V2_07 VAŠOVÁ, Sabína - BENKA, Denis - KEBÍSEK, Michal - STRÉMY, Maximilián. Detection of Landcover Using Convolutional Neural Network. In *Machine Learning Methods in Systems. CSOC 2024. Volume 4*. 1. vyd. Cham : Springer Nature, 2024, s. 94-105. ISSN 2367-3370. ISBN 978-3-031-70594-6 (2023: 0.171 - SJR, Q4 - SJR Best Q). V databáze: DOI: 10.1007/978-3-031-70595-3_12 ; SCOPUS: 2-s2.0-85208626513.
Typ výstupu: príspevok z podujatia; Výstup: zahraničný; Kategória publikácie do 2021: AFC

V3 Vedecký výstup publikačnej činnosti z časopisu

V3_01 BENKA, Denis - VAŠOVÁ, Sabína - KEBÍSEK, Michal - STRÉMY, Maximilián. Detection of a Quasiperiodic Phenomenon of a Binary Star System Using Convolutional Neural Network. In *Intelligent Automation & Soft Computing*. Vol. 37, iss. 3 (2023), s. 2519-2535. ISSN 1079-8587 (2023: 0.338 - SJR, Q3 - SJR Best Q). V databáze: DOI: 10.32604/iasc.2023.040799 ; SCOPUS: 2-s2.0-85172265058.
Typ výstupu: článok; Výstup: zahraničný; Kategória publikácie do 2021: ADM

V3_02 DOBROTKA, Andrej - ORIO, M. - BENKA, Denis - VANDERBURG, A. Searching for the 1 mHz variability in the flickering of V4743 Sgr: A cataclysmic variable accreting at a high rate. In *Astronomy & Astrophysics*. Vol. 649, (2021), s. 1-5. ISSN 0004-6361 (2021: 6.240 - IF, Q1 - JCR Best Q, 1.918 - SJR, Q1 - SJR Best Q). V databáze: DOI: 10.1051/0004-6361/202039742 ; WOS: 2-s2.0-85105880579 ; CC: 000655638100001.
Typ výstupu: článok; Výstup: zahraničný; Kategória publikácie do 2021: ADC

Ohlasy:

1. [1] FEIGELSON, Eric D. - BIANCO, Federica B. - BONITO, Rosaria. An Evenly Spaced LSST Cadence for Rapidly Variable Stars. In: Astrophysical Journal, Supplement Series, 2023-09-01, 268, 1, pp. ISSN 00670049., Registrované v: SCOPUS, WOS, CC
Ohlas: zahraničný

V3_03 HORVÁTH, Dušan - HERCHLOVÁ, Monika - BENKA, Denis - STRÉMY, Maximilián. Kybernetické hrozby v priemyselných riadiacich systémoch. In *AT&P Journal*. Roč. 31, č. 1 (2024), s. 36-37. ISSN 1335-2237.
Typ výstupu: článok; Výstup: domáci; Kategória publikácie do 2021: ADE

V3_04 BENKA, Denis – HORVÁTH, Dušan – ŠPENDLA, Lukáš – GAŠPAR, Gabriel – STRÉMY Maximilián. Machine Learning-Based Detection of Anomalies, Intrusions and Threats in Industrial Control Systems. In *IEEE Access*. 2025.
Typ výstupu: článok; Výstup: zahraničný; Kategória publikácie do 2021: ADC. Stav: akceptované

O2 Odborný výstup publikačnej činnosti ako časť knižnej publikácie alebo zborníka

O2_01 DOBROTKA, Andrej - BEZÁK, Pavol - MAGDOLEN, Jozef - BENKA, Denis. Fast variability in accretion systems research group. In *Bulletin vedeckých príspevkov : Bulletin vedeckých príspevkov z projektu Vedeckovýskumné centrum excelentnosti Slovakion pre materiálový a interdisciplinárny výskum*. 1. vyd. Bratislava : Spektrum, 2022, S. 35-40. ISBN 978-80-227-5220-6.
Typ výstupu: príspevok; Výstup: domáci; Kategória publikácie do 2021: BEF