UNIVERSITY OF ŽILINA
Faculty of Electrical Engineering and Information Technology

Téma dizertačnej práce (DzP)

Akademický rok *2026/2027*

Názov	**Zvyšovania kybernetickej odolnosti OT systémov.**		
Inštitúcia	Fakulta elektrotechniky a informačných technológií Žilinská univerzita v Žiline		
Miesto	Žilina, Slovensko		
PhD. program	Riadenie procesov		
Školiteľ	prof. Ing. Rastislav Pirník, PhD., Katedra riadiacich a informačných systémov		
Školiteľ špecialista			
Forma štúdia	Denná		
Dĺžka štúdia	3 roky		
Jazyk štúdia	Slovenský		
Dátum nástupu	1.9.2026		
Výskumná oblasť	Kybernetika		
Kontakt zadávateľa	Tel. číslo:	E-mail:	Web stránka:
	+421 41 513 3351	rastislav.pirnik@uniza.sk	link

Anotácia témy DzP

Navrhovaná dizertačná práca sa zameriava na preskúmanie, modelovanie a zvýšenie kybernetickej odolnosti systémov operačných technológií (OT) v prostredí kritickej infraštruktúry. Digitalizácia priemyselných procesov a konvergencia IT/OT prostredí významne zvyšujú mieru vystavenia priemyselných riadiacich systémov kybernetickým hrozbám. Incidenty ako útok na Colonial Pipeline, malware Stuxnet či Industroyer poukazujú na potrebu systematického prístupu ku kybernetickej odolnosti OT systémov.

Cieľom práce je navrhnúť metodiku hodnotenia a adaptívneho zvyšovania kybernetickej odolnosti OT systémov, ktorá bude zohľadňovať špecifiká priemyselných riadiacich systémov (ICS), fyzikálne dopady kybernetických incidentov a požiadavky na bezpečnosť, dostupnosť a kontinuitu prevádzky. Súčasťou riešenia bude modelovanie hrozieb, kvantifikácia odolnosti pomocou definovaných metrík (napr. MTTD, MTTR, index prevádzkovej kontinuity), návrh architektonických a procesných opatrení a experimentálna validácia na testovacom alebo simulovanom OT prostredí.

Výsledkom práce bude originálny **model alebo framework** umožňujúci systematické hodnotenie a optimalizáciu kybernetickej odolnosti OT systémov s potenciálnym využitím v energetike, priemyselnej výrobe, doprave a ďalších sektoroch kritickej infraštruktúry.

Rozšírené informácie, výskumné zodpovednosti a úlohy doktoranda

Doktorand bude riešiť výskumnú úlohu zameranú na návrh vedecky podloženej metodiky hodnotenia a zvyšovania kybernetickej odolnosti OT systémov v súlade s medzinárodnými štandardmi, ako sú rámce NIST Cybersecurity Framework a norma IEC 62443.

Hlavné výskumné úlohy:

Analýza súčasného stavu poznania

- systematický prehľad literatúry v oblasti resilience engineering a bezpečnosti ICS/SCADA,
- identifikácia existujúcich modelov hodnotenia odolnosti,
- analýza legislatívnych a normatívnych požiadaviek.

Definovanie modelu kybernetickej odolnosti OT:

- návrh formálnej definície kybernetickej odolnosti OT systémov,
- identifikácia kľúčových metrík a parametrov hodnotenia,
- modelovanie závislostí medzi kybernetickou a fyzikálnou vrstvou systému.

Návrh metodiky hodnotenia a optimalizácie:

- návrh kvantifikačného modelu (napr. na báze pravdepodobnostných alebo simulačných prístupov),
- vytvorenie hodnotiaceho frameworku (resilience scoring model),
- návrh adaptívnych opatrení na zvýšenie odolnosti (segmentácia siete, detekčné mechanizmy, redundancia, bezpečnostné architektúry).

Experimentálna validácia:

- návrh a implementácia experimentálneho OT testbedu alebo digitálneho dvojčaťa,
- simulácia vybraných typov útokov,
- vyhodnotenie dopadu bezpečnostných opatrení na úroveň odolnosti.

Publikačná a vedecká činnosť:

- publikovanie výsledkov vo vedeckých časopisoch a na medzinárodných konferenciách,
- aktívna účasť na grantových projektoch a výskumných aktivitách pracoviska.

Doktorand bude zodpovedný za samostatné riešenie vedeckých úloh, návrh metodických postupov, realizáciu experimentov, analýzu výsledkov a formulovanie vedeckých záverov.

Profil uchádzača

Odborné znalosti:

- základy kybernetickej bezpečnosti (network security, risk management),
- znalosť architektúr IT a OT systémov,
- orientácia v problematike priemyselných riadiacich systémov (ICS, SCADA, PLC),
- základná znalosť bezpečnostných štandardov (napr. IEC 62443, NIST CSF),
- schopnosť pracovať s modelovacími alebo simulačnými nástrojmi.

Technické zručnosti:

- pokročilá znalosť sieťových technológií,
- skúsenosti s virtualizáciou alebo laboratórnym testovaním,
- programovanie (napr. Python, MATLAB, alebo iný analytický nástroj),
- schopnosť pracovať s dátovou analýzou a štatistickými metódami.

Vedecké predpoklady:

- schopnosť samostatnej vedeckej práce,
- analytické a kritické myslenie,
- schopnosť formulovať výskumné otázky a hypotézy,
- dobrá znalosť anglického jazyka (písomná aj ústna forma),
- predpoklad publikovania vo vedeckých časopisoch.

Výhodou je:

- prax v oblasti OT bezpečnosti alebo priemyselnej automatizácie,
- skúsenosť s penetračným testovaním alebo bezpečnostným auditom,
- účasť na výskumných alebo bezpečnostných projektoch.

Požadované vstupy vo forme HW a SW boli zabezpečené z projektu MATCHING (prvá fáza). Predpokladané náklady na diseminácu výsledkov plánujeme pokryť aktívnym zapojením do rôznych projektov, či už na úrovni fakulty, univerzity, alebo neskôr podaných projektov VEGA, KEGA, APVV, respektíve HORIZON Europe.