Mithril

Cyber-Physical Digital Twin for Flexibility, Cybersecurity, and Grid Resilience in Modern Power Systems

Programm / Ausschreibung	EW 24/26, CETP 2025, CETPartnership JC 2025 (EW)	**Status**	laufend
Projektstart	01.12.2026	**Projektende**	30.11.2029
Zeitraum	2026 - 2029	**Projektlaufzeit**	36 Monate
Barwert der Projektförderung	€ 430.356		
Keywords	Cyber-Physical Systems; Digital Twin; Smart Grids; Grid Flexibility; Resilience; Cybersecurity; Co-Simulation; Distributed Energy Resources (DER); Virtual Power Plant (VPP); Data-in-the-Loop; Intrusion Detection; Semantic Modeling; Interoperability;		

Projektbeschreibung

Ausgangslage und Motivation: Europäische Verteilnetze wandeln sich zu komplexen cyber-physischen Systemen mit rasch wachsendem Anteil dezentraler erneuerbarer Energieressourcen (DER). Bis 2050 wird laut Europäischer Kommission eine bis zu siebenfach höhere Flexibilitätskapazität benötigt. Diese muss durch koordinierte Solar-PV-Anlagen, Batteriespeicher, Elektrofahrzeuge und Demand Response bereitgestellt werden. Die Integration von Millionen solcher Ressourcen erzeugt jedoch erhebliche Cybersicherheitsrisiken und operationelle Komplexität. Der ENISA Threat Landscape Report 2024 weist Energiesysteme als einen der fünf am stärksten von Cyberangriffen betroffenen Sektoren aus (+38 % gemeldete Vorfälle). Die NIS2-Richtlinie (EU 2022/2555) unterstreicht den dringenden Bedarf an validierten Werkzeugen für cyber-resilienten Netzbetrieb. Gleichzeitig fehlen systematische Testumgebungen, die das Zusammenspiel von physischer Netzinfrastruktur, IKT-Systemen und Steuerungslogik unter realistischen Bedingungen einschließlich Cyberangriffen ganzheitlich abbilden. Herkömmliche Offline-Simulationen und isolierte Hardware-in-the-Loop-Tests erfassen weder kaskadierende Wechselwirkungen noch Cybersicherheitsabhängigkeiten moderner Verteilnetze.

Ziele und Innovationsgehalt: MITHRIL entwickelt eine containerisierte Co-Simulationsplattform auf Basis von Kubernetes als cyber-physischer digitaler Zwilling für die Validierung von Netzflexibilität, Cybersicherheit und Resilienz. Vier synergetische Ziele werden verfolgt: (O1) eine skalierbare, durch semantische Modelle (CIM, IEC 61850) und LLM-basierte Agenten orchestrierte Simulationsumgebung mit HPC-Fähigkeit für Monte-Carlo-Kampagnen (>10.000 Szenarien); (O2) sichere DER-Koordination mittels Multi-Agenten Deep Reinforcement Learning mit projektionsbasierten Sicherheitsgarantien für harte Einhaltung von Spannungs- und thermischen Grenzen; (O3) ein modulares Cybersicherheits-Toolkit mit umfassender Angriffstaxonomie (physisch, klassisch-cyber, KI-basiert), digitaler-Zwilling-basierter Anomalieerkennung und Wirkungsquantifizierung gemäß IEC 62351/NIS2; sowie (O4) Demonstration eines TRL-6-Prototyps mit Operator-in-the-Loop-Übungen bei GDZ İzmir. Der zentrale Innovationsgehalt liegt in der erstmaligen Kombination von semantisch gesteuerter Automatisierung, LLM-unterstützter natürlichsprachlicher Szenariospezifikation, Kubernetes-basierter elastischer Skalierung

und integrierter Cyber-Physical-Angriffssimulation in einer einzigen Plattform.

Erwartete Ergebnisse: mMITHRIL liefert: (1) eine Open-Source-Co-Simulationsplattform mit automatisierter Konfiguration und reproduzierbaren containerisierten Testumgebungen; (2) validierte DRL-Algorithmen mit garantierter Einhaltung von Netzrestriktionen (>99,9 % Constraint-Erfüllung über 1.000 Testszenarien); (3) ein Cybersicherheits-Assessment-Toolkit mit automatisierter Generierung mehrstufiger Angriffsszenarien und mehrdimensionalem Resilienz-Score; (4) einen bei GDZ İzmir demonstrierten TRL-6-Prototyp mit quantifizierten Verbesserungen bei Erkennungsgenauigkeit und Reaktionszeit, validiert durch kognitive Belastungsmessungen; sowie (5) replizierbare Referenzarchitekturen, Schulungsmaterialien und Politikempfehlungen. Das transnationale Konsortium aus sechs Partnern in Österreich, Schweden und der Türkei deckt die Innovationskette von TRL 3 bis TRL 6 in 36 Monaten ab, gesteuert durch phasenbasierte Go/No-Go-Entscheidungspunkte.

Abstract

Background and Motivation: European distribution grids are rapidly evolving into complex cyber-physical systems with a growing share of distributed energy resources (DER). By 2050, the European Commission projects that up to seven times greater flexibility capacity will be needed to meet climate neutrality targets. This flexibility must come from coordinated solar PV, battery storage, electric vehicles, and demand response. However, integrating millions of such resources creates significant cybersecurity vulnerabilities and operational complexity that existing grid management systems cannot address. The ENISA Threat Landscape Report 2024 identifies energy systems among the five infrastructure sectors most targeted by cyber-adversaries (+38% reported incidents). The NIS2 Directive (EU 2022/2555) underscores the urgent need for validated tools enabling cyber-resilient grid operation. At the same time, systematic testing environments capable of holistically capturing the interplay between physical grid infrastructure, ICT systems, and control logic under realistic conditions — including cyberattacks — are lacking. Conventional offline simulations and isolated hardware-in-the-loop tests fail to capture cascading interdependencies and cybersecurity vulnerabilities of modern distribution grids.

Goals and Innovation Content: MITHRIL develops a containerized co-simulation platform based on Kubernetes serving as a cyber-physical digital twin for validating grid flexibility, cybersecurity, and resilience. Four synergistic objectives are pursued: (O1) a scalable simulation environment orchestrated by semantic models (CIM, IEC 61850) and LLM-based agents with HPC capability for Monte Carlo campaigns (>10,000 scenarios); (O2) safe DER coordination via multi-agent deep reinforcement learning with projection-based safety guarantees enforcing hard compliance with voltage and thermal limits; (O3) a modular cybersecurity toolkit with a comprehensive attack taxonomy (physical, classical cyber, AI-based), digital-twin-based anomaly detection, and impact quantification aligned with IEC 62351/NIS2; and (O4) demonstration of a TRL 6 prototype through operator-in-the-loop exercises at GDZ İzmir. The core innovation lies in the first-ever combination of semantically driven automation, LLM-assisted natural-language scenario specification, Kubernetes-based elastic scaling, and integrated cyber-physical attack emulation within a single platform.

Expected Results: MITHRIL delivers: (1) an open-source co-simulation platform with automated configuration and reproducible containerized test environments; (2) validated DRL algorithms with guaranteed compliance with grid constraints (>99.9% constraint satisfaction across 1,000 test scenarios); (3) a cybersecurity assessment toolkit with automated generation of multi-stage attack scenarios and a multi-dimensional resilience score; (4) a TRL 6 prototype demonstrated at GDZ İzmir with quantified improvements in operator detection accuracy and response time, validated through cognitive workload measurements; and (5) replicable reference architectures, training materials, and policy

recommendations. The transnational consortium of six partners in Austria, Sweden, and Turkey covers the full innovation chain from TRL 3 to TRL 6 within 36 months, governed by phased Go/No-Go decision gates.

Projektpartner

- AIT Austrian Institute of Technology GmbH