

# GRADUATE RESEARCH PROPOSAL

## Project Title:

## GenAI-Driven Resilient Control and Anomaly Detection in Cyber-Physical Systems

### Project Summary:

This research enhances the security and operational resilience of Cyber-Physical Systems (CPS)—such as autonomous surface vessels, robotics, and critical energy grids—against stealthy adversarial cyber attacks and dynamic environmental anomalies. By synthesizing control theory, cybersecurity, and Generative AI (GenAI), this framework develops real-time threat detection, automated attack scenario generation, and adaptive control recovery strategies. GenAI architectures—including Generative Adversarial Networks (GANs), Diffusion Models, and LLM-driven decision agents—are leveraged to synthesize zero-day threat vectors, reconstruct compromised sensor signals, and automate dynamic control stabilization under severe operational uncertainty.

### Project Details:

Cyber-Physical Systems (CPS) tightly integrate computing, communication, and physical dynamics. However, increased network connectivity exposes CPS to sophisticated cyber attacks (e.g., false data injection, denial-of-service, replay attacks) that compromise sensor telemetry and degrade physical safety.

This research focuses on four key technical modules:

1. **Generative Threat Modeling & Synthetic Attack Synthesis:** Formulate dynamic game-theoretic attack models. Utilize Deep Generative Models (GANs, VAEs) to synthesize realistic, unencountered zero-day attack scenarios and extreme edge cases, stress-testing CPS resilience beyond historical datasets.
2. **Real-Time AI-Driven Anomaly Detection:** Combine model-based observers (Kalman filters, Luenberger observers) with Transformer-based sequence-to-sequence reconstruction models. The framework reconstructs non-corrupted state distributions in real time to isolate stealthy data injection attacks with ultra-low false alarm rates.
3. **Resilient Estimation & Generative Control Adaptation:** Integrate Generative Diffusion Models with Model Predictive Control (MPC) to infer missing or corrupted telemetry trajectories. The system generates real-time adaptive control signals to maintain physical stability under active compromise.
4. **Intelligent Response via Generative Reinforcement Learning:** Deploy Deep Reinforcement Learning (RL) guided by generative agent frameworks to execute automated threat response planning, continuously adapting strategies through real-time physical feedback.

### Expected Deliverables:

- A generative simulation framework for CPS zero-day threat synthesis and vulnerability assessment.
- Open-source, real-time GenAI anomaly detection and adaptive control toolkits validated on MATLAB/Simulink and Hardware-in-the-Loop (HIL) testbeds.
- Reproducible synthetic CPS benchmark datasets for the scientific community.
- High-impact publications in peer-reviewed journals (e.g., IEEE, ACM, Springer).

### Research Methods:

The methodology integrates system dynamics, state-space modeling, stochastic game theory, and deep generative modeling. Initial validation will be conducted in MATLAB/Simulink simulation environments, followed by physical hardware-in-the-loop (HIL) experimentations (e.g., micro-grid and autonomous surface vessel testbeds).

## References Cited

- Ding, D., Han, Q.L., Xiang, Y., Ge, X. and Zhang, X.M., 2018. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, 275, pp.1674–1683. Available at: <https://doi.org/10.1016/j.neucom.2017.10.009> [Accessed 7 May 2025].
- Giraldo, J., Sarkar, E., Cardenas, A.A., Maniatakos, M. and Kantarcioglu, M., 2018. A survey of physics-based attack detection in cyber-physical systems. *ACM Computing Surveys*, 51(4), pp.1–36. Available at: <https://doi.org/10.1145/3203245> [Accessed 7 May 2025].
- Mitchell, R. and Chen, I.R., 2014. A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys*, 46(4), pp.1–29. Available at: <https://doi.org/10.1145/2542049> [Accessed 7 May 2025].
- Mo, Y., Chabukswar, R., Sinopoli, B., Dawson, C., Koutsoukos, X. and Sastry, S., 2012. Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1), pp.195–209. Available at: <https://doi.org/10.1109/JPROC.2011.2161428> [Accessed 7 May 2025].
- Pasqualetti, F., Dörfler, F. and Bullo, F., 2013. Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 58(11), pp.2715–2729. Available at: <https://doi.org/10.1109/TAC.2013.2266831> [Accessed 7 May 2025].
- Shahriari-Kahkeshi, M., Alem, S.A. and Shi, P., 2024. Detection, reconstruction and mitigation of deception attacks in nonlinear cyber-physical systems. *International Journal of Adaptive Control and Signal Processing*, 38(10), pp.3411–3430. Available at: <https://doi.org/10.1002/acs.3854> [Accessed 7 May 2025].
- Teixeira, A., Shames, I., Sandberg, H. and Johansson, K.H., 2015. A secure control framework for resource-limited adversaries. *Automatica*, 51, pp.135–148. Available at: <https://doi.org/10.1016/j.automatica.2014.10.067> [Accessed 7 May 2025].
- Yan, B., Shi, P., Karimi, H.R. and Lim, C.P., 2024. Event and learning-based resilient formation control for multiagent systems under DoS attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 54(8), pp.4876–4886. Available at: <https://doi.org/10.1109/TSMC.2024.3400879> [Accessed 7 May 2025].
- Yan, B., Shi, P. and Chambers, J., 2024. Cooperative control for heterogeneous multi-agent systems: progress, applications, and challenges. *Science China Information Sciences*, 67(5), pp.156201-1–156201-3. Available at: <https://doi.org/10.1007/s11432-024-4001-6> [Accessed 7 May 2025].
- Zhang, Y., Wang, L., Liu, Y. and Zhang, P., 2019. Cyber physical security analytics for transactive energy systems. *IEEE Transactions on Smart Grid*, 11(2), pp.931–941. Available at: <https://doi.org/10.1109/TSG.2019.2928168> [Accessed 7 May 2025].