SEMICONDUCTORS & MICROELECTRONICS
SECURITY AND AUTOMATION

University of Arizona researchers advance the security and reliability of hardware, embedded, and cyber-physical systems through artificial intelligence (AI)-driven modeling, design, and verification. Their work leverages machine learning (ML) to construct digital twins—comprehensive system models that enable detection of attacks, failures, and security threats. They develop scalable solutions to automate design and verification, addressing the growing complexity of next-generation microelectronics.

Hardware security

The rapid growth in hardware complexity and time-to-market demands has led to globalization of the semiconductor supply chain, introducing significant security vulnerabilities throughout the integrated circuit (IC) lifecycle. Outsourcing critical stages—such as design, fabrication, and testing—to untrusted third parties exposes hardware to threats, including intellectual property (IP) piracy, side-channel attacks, and malicious modifications like hardware Trojans. These risks compromise the confidentiality, integrity, and reliability of microelectronic systems across defense, infrastructure, and commercial sectors.

The team uses automated, AI-driven, and context-aware methodologies that span both design time and runtime. Circuit designs are encoded as heterogeneous graphs and analyzed using Graph Neural Networks to detect and localize hardware Trojans and IP theft without relying on golden reference chips or manual inspection. For post-silicon protection, the team develops ML and brain-inspired models to analyze power and electromagnetic side-channel emissions, identifying malicious activity during chip operation. The team also uncovers vulnerabilities in hardware and systems in modern computing platforms. Together, these efforts form scalable, multidisciplinary frameworks for securing current and next-generation semiconductor systems from the ground up.

AI-driven automation of design & verification

The team leverages generative AI to automate the design and verification of hardware. By modeling circuits and systems as structured data, these techniques can accurately predict performance metrics, identify vulnerabilities, and guide design decisions. This approach significantly reduces the time and complexity of design and verification while improving reliability and scalability. As microelectronics grow increasingly heterogeneous and intricate, AI-driven automation provides a robust, adaptable framework to meet the demands of next-generation technologies.

Cyber-physical systems security

The growing reliance on cyber-physical systems in critical domains, such as healthcare and industrial automation, has amplified the urgency to ensure security and reliability. These systems face unique vulnerabilities due to physical sensing and cyber layer integration. The team addresses these challenges through the multi-modal anomaly detection approach that fuses sensor and communication data into a unified knowledge graph. Leveraging graph neural networks, the model learns operational context and detects deviations indicative of failures or attacks. This integrated strategy demonstrated significant performance gains over single-domain models, enabling more accurate, robust, and timely detection of abnormal behaviors. By unifying physical and cyber intelligence, these methods advance the security and adaptability of embedded and cyber-physical systems in increasingly complex environments.

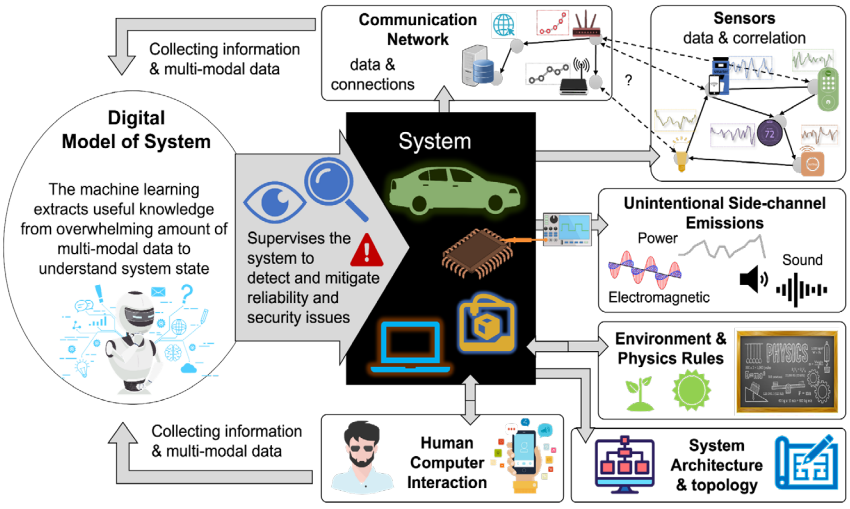

Figure: Digital twin model overview. Our models integrate disparate sources of information and extract practical knowledge to understand and supervise systems.

Rozhin Yasaei, PhD | Assistant Professor
Information Science | yasaei@arizona.edu

Rozhin focuses on security and design automation for hardware and cyber-physical systems, leveraging applied machine learning. She leverages Graph Neural Networks and other cutting-edge methodologies to model these systems.

More information:

R. Yasaei et al., GNN4IP: Graph Neural Network for Hardware Intellectual Property Piracy Detection. *ACM/IEEE Design Automation Conference* (2021). doi: 10.1109/DAC18074.2021.9586150