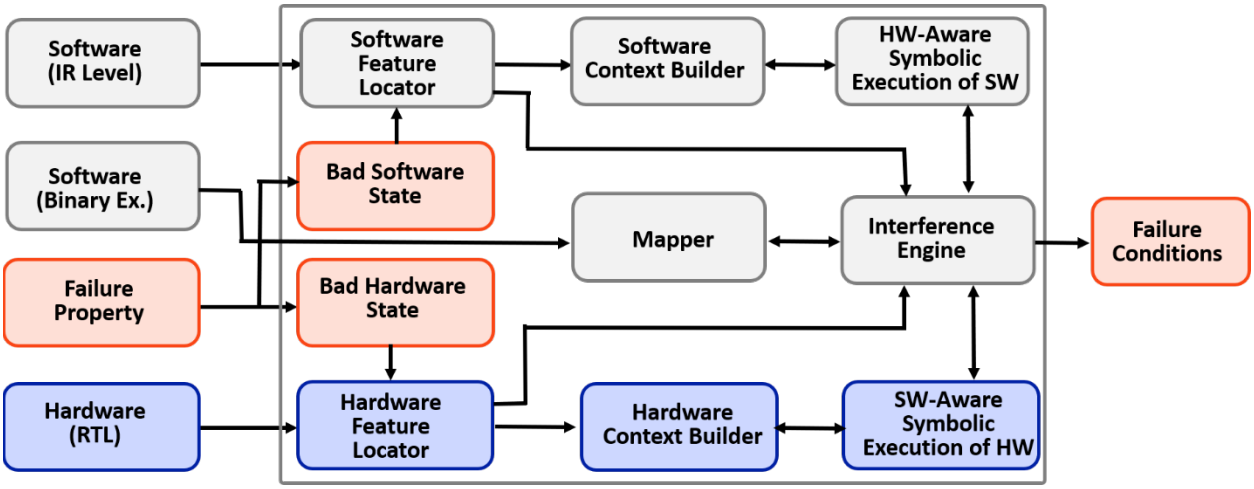
Reusable hardware Intellectual Property (IP) based System-on-Chip (SoC) design has emerged as a pervasive design practice in the industry today. The possibility of hardware Trojans and/or design backdoors hiding in IP cores has raised security concerns. Formal methods have shown their importance in exhaustive hardware security verification, but few of them provide an effective solution in the following three scenarios: software and hardware boundary, large scale SoC designs, and runtime verification. On the other hand, hardware vulnerabilities are often due to design mistakes or formed by the analog circuit properties of underlying circuits. Motivated by the above concerns, **research in K-State Hardware Security Lab mainly focused on developing methods for ensuring security and trustworthiness of integrated circuits and systems** and has contributed several key solutions that have been widely acknowledged and referenced by the newly emerging scientific community in the area of trusted hardware.

NSF Funded Project: Property-specific Hardware-oriented Formal Verification Modules for Embedded Systems.

This project investigates a property-driven approach to hardware software co-verification. Things unique to their approach include a property-directed co-model extraction and a property-specific run-time validation process to achieve scalability and precision in detecting bugs due to hardware-software interactions. Specifically, two categories of hardware software interactions are considered: 1) hardware as the executor of software and 2) hardware and software acting as cooperating entities.

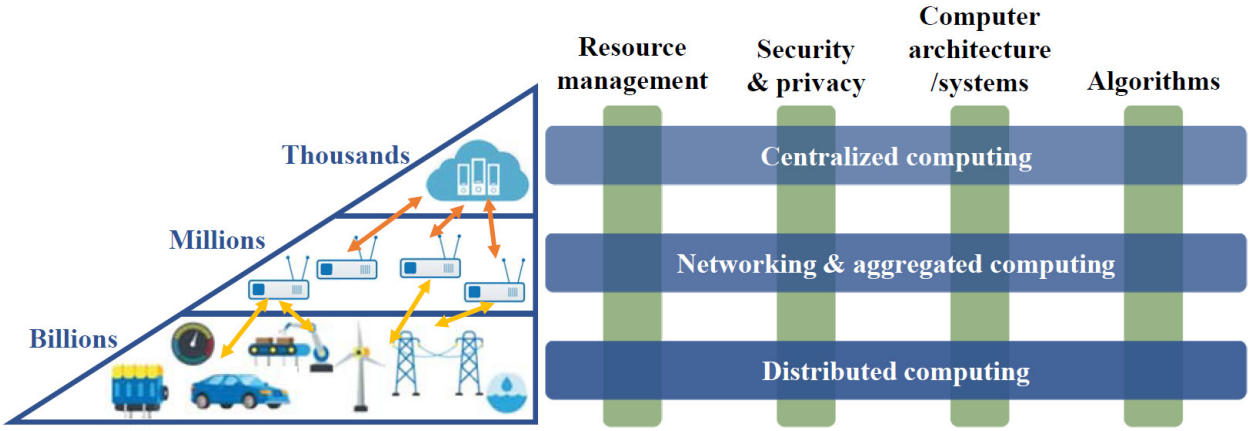
The work of this project will develop novel hardware software co-verification techniques and tools. It will have a significant impact in the reliability and the security of the Internet of Things. Dr Guo and his team are leveraging the developed artifacts for training a workforce that is equipped with the cutting edge embedded system development and verification skills. The developed benchmarks will foster collaboration with the industry and serve other researchers in the area.



NSF Funded Project: S3-IoT: Design and Deployment of Scalable, Secure, and Smart Mission-Critical IoT Systems.

The increasing number of IoT devices along with their growing heterogeneity of compilation and architecture platforms raise the challenges of achieving security and privacy assurance. Novel techniques including formal verification for protocol trustworthiness, and information flow tracking for privacy-preserving are investigated and their implementation in scalable IoT are assessed.

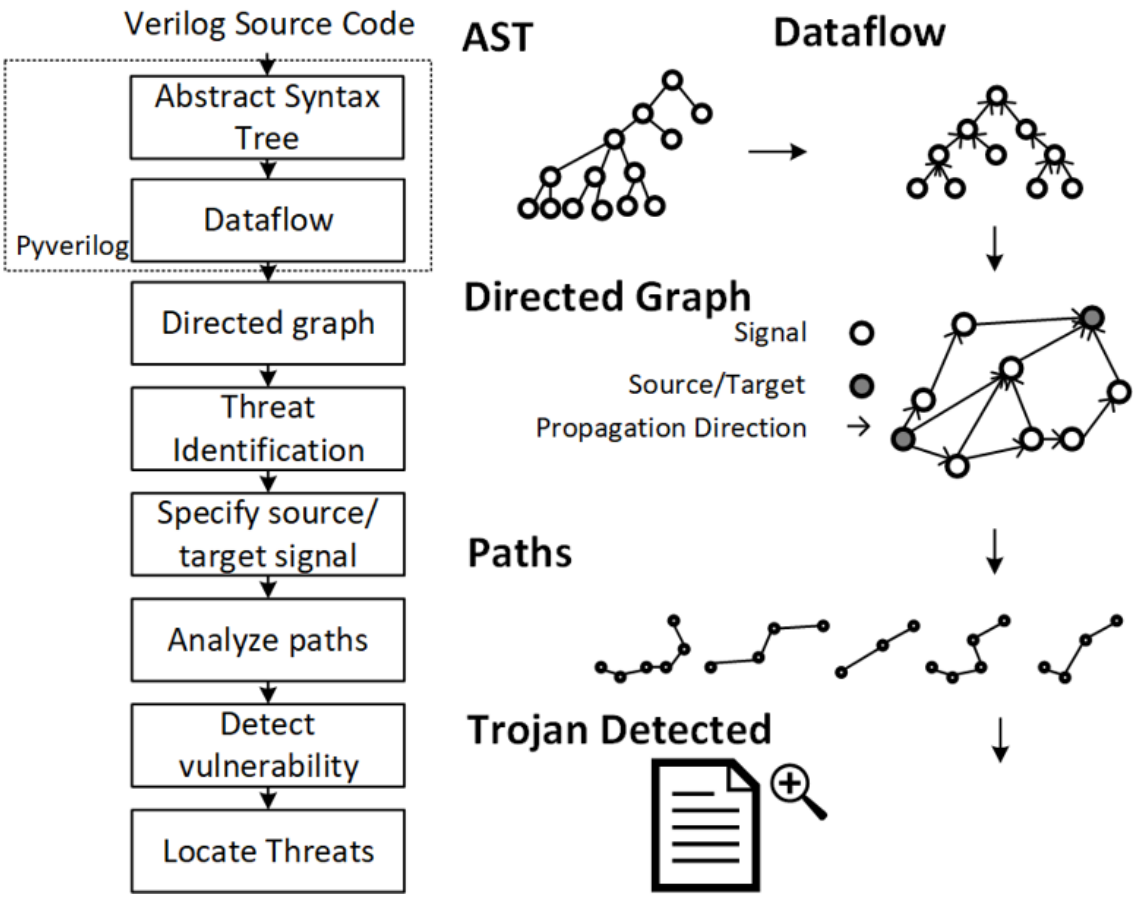
This project generates transformative innovations for designing scalable, secure and smart hardware systems, like IoT systems, through the proposed framework. From the security and privacy angle, scalable and resilient security solutions are investigated for analyzing vulnerabilities of scaled hardware systems. This research outcomes have broader impacts on the deployment of large-scale, mission-critical IoT systems and infrastructures, particularly in terms of improving resilience to design errors and malicious attacks.



RTL level Security Analysis via Information Flow Tracking

The use of third party hardware IP enables fast development of new electronic systems and is prevalent today in both commercial and defense applications. However, untrusted third-party vendors and off-shore foundries are involved in the IC supply chain, which raises security and trustworthiness concerns. The breaking news of a suspicious hardware Trojan insertion in the SuperMicro board is a typical example of threats from untrusted third-parties. Therefore, scalable and low cost methods for ensuring that no malicious functionality is included in the third-party hardware IP are needed.

Information flow tracking (IFT) is a security technique that tracks the tainted data objects to record information propagation and detect security violations. This project proposes a framework that applies IFT to detect hardware Trojans or vulnerabilities on a System-on-Chip (SoC) system. In the framework, a suspicious data flow is tracked based on HDL code while the propagation constrains are extracted and analyzed from the targeted system. This technique helps IP design house to identify specific threats from their design and verify the integrity and confidentiality of the SoC.


Verilog Source Code
Abstract Syntax Tree
Dataflow
Pyverilog
Directed graph
Threat Identification
Specify source/ target signal
Analyze paths
Detect vulnerability
Locate Threats
AST
Dataflow
Directed Graph
Signal
Source/Target
Propagation Direction
Paths
Trojan Detected