



Bridging Hardware and Software Through Causality Inference

Zhaoxiang Liu*, Kejun Chen*, Dean Sullivan†, Orlando Arias‡, Xiaolong Guo*

*Kansas State University {zxliu, kejun, guoxiaolong}@ksu.edu †University of New Hampshire dean.sullivan@unh.edu

‡University of Massachusetts Lowell orlando_arias@uml.edu



Background & Motivations

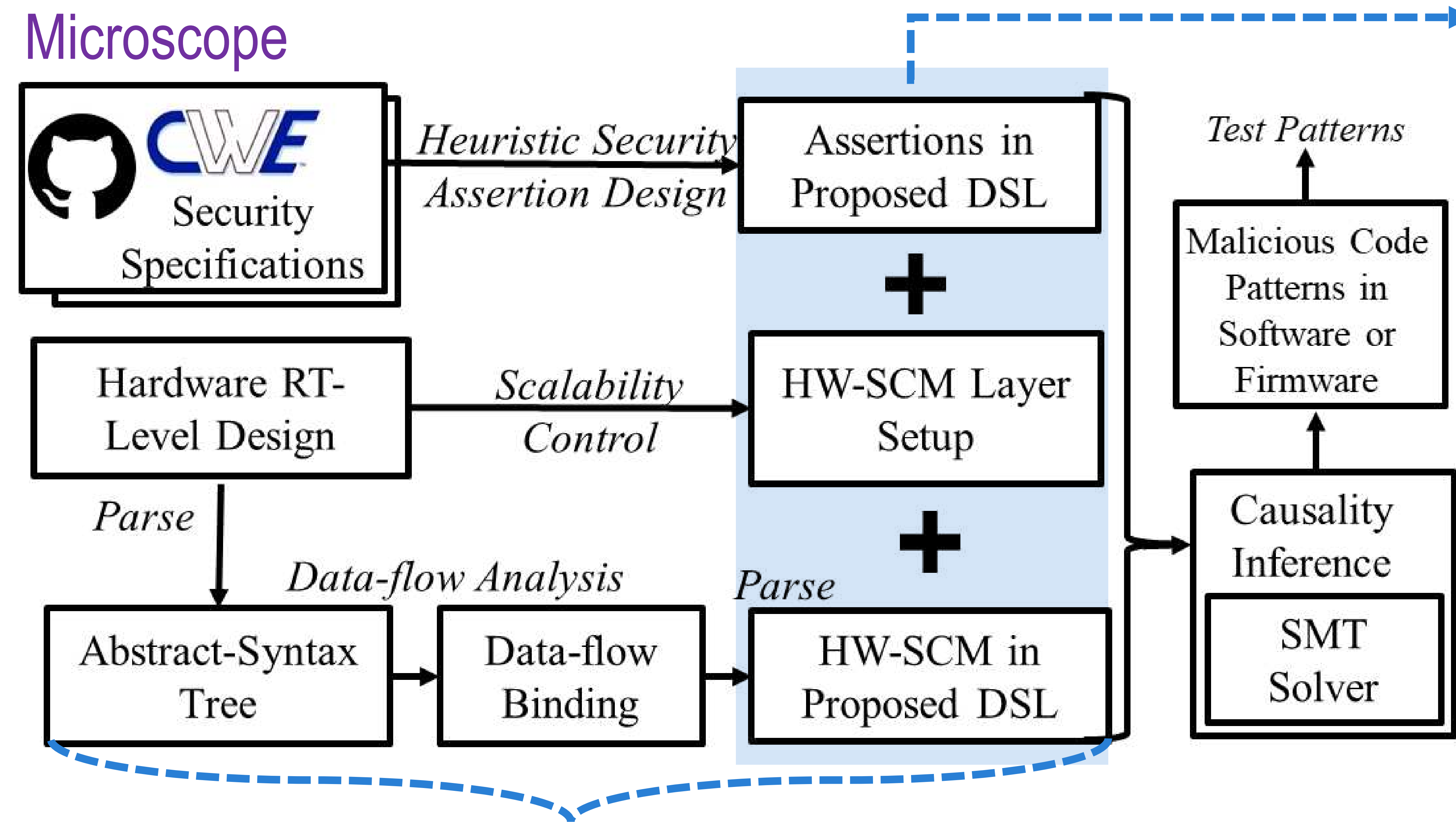
System-on-chip (SoC) security concerns:

- Globalization of supply chain: IC Life cycle exposes risk
- Complexity of SoC: the increasing manual workload
- Software-exploited hardware bugs present rigorous challenges

Contributions

- The Hardware Structural Causal Model (HW-SCM) to model hardware and software together.
- A domain-specific language (DSL) in SMT-LIB 2 representing HW-SCM.
- Microscope [1]: use HW-SCM to infer potential software instruction patterns that expose hardware vulnerabilities.

Microscope



Structural Causal Model & HW-SCM

Causality Inference: Reason cause-and-effect relationships between variables.

Structural causal model (SCM): Describe the relevant features of the world and how they interact with each other.

- **HW-SCM:** Model the causality among hardware signals and software instructions:

$$f_{comb} = \{f_i: X_i \rightarrow y_i \mid y_i \in HW_i\}$$

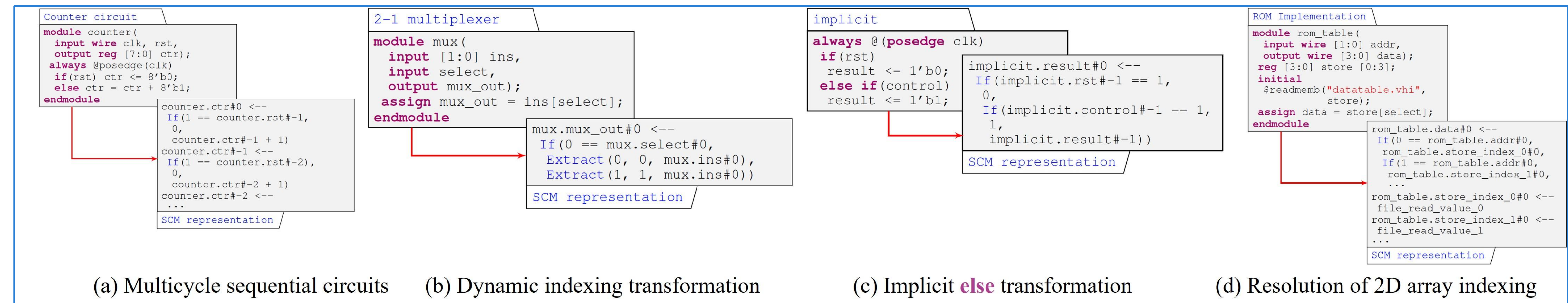
$$f_{seq} = \{f_i: X_{i-1} \rightarrow y_i \mid y_i \in HW_i\}$$

f_{comb} : capture the combinational dependencies

f_{seq} : capture the sequential dependencies

HW_i : the set of hardware signals (excluding the inputs)

HW-SCM in SMT LIB2



Experiment & Comparison

Implementation & Environment

- Developed by Python & Microsoft Z3 as SMT solver

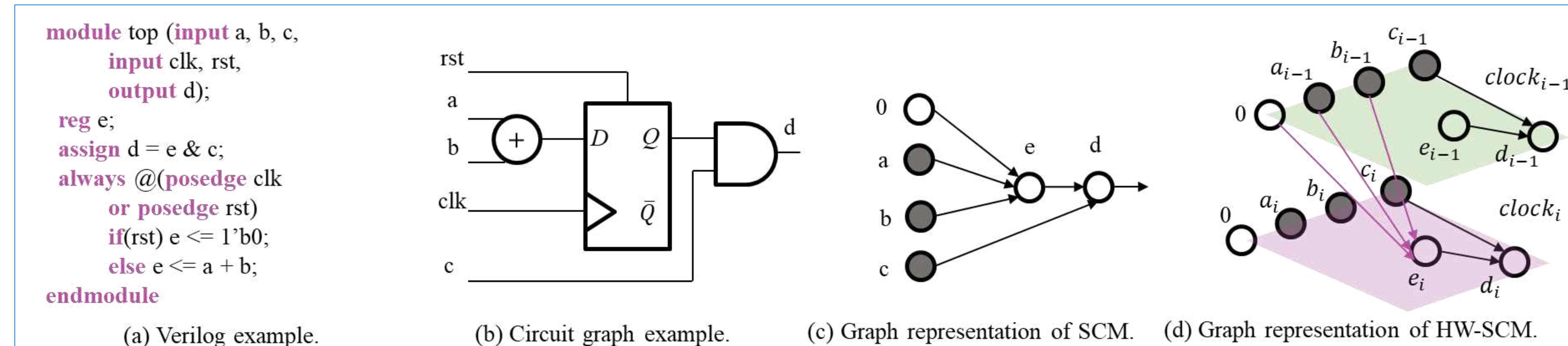
Benchmark evaluations

- DarkRISC-V, RISC-V-Mini, OR1200

Comparison with Coppelia and JasperGold FPV

- OR1200 testbench and Bugzilla dataset

Tools	Time	Replay	Traces
Coppelia	252s	Yes	≥1
FPV	0.1s	No	1
MicroScope	21.72s	Yes	≥1



Denotes in the graph representations	Hardware behaviors
Multi-layer	Each layer represent one specific time slot
Arrowhead	The direction of signal propagation
Endogenous node	Hardware signal
Exogenous node	Software instruction/input
In-layer connection	Combinational assignment
Cross-layer connection	Sequential assignment



[1] Liu, Zhaoxiang, Kejun Chen, Dean Sullivan, Orlando Arias, Raj Gautam Dutta, Yier Jin, and Xiaolong Guo. "Microscope: Causality Inference Crossing the Hardware and Software Boundary from Hardware Perspective."

In *Proceedings of the ASPDAC Asia and South Pacific Design Automation Conference*. 2024.

NEWHS 2024 | 5 April 2024

Portions of this work were supported by the National Science Foundation (CCF-2019310, First Award Program of ARISE in EPSCoR 2148878).