Safety Verification of Third-Party Hardware Modules via Information Flow Tracking

Andres Meza, Francesco Restuccia, Ryan Kastner, and Jason Oberg

In a Nutshell

- Introduce the AXI bus stall problem
- Propose a safety verification methodology to identify the AXI bus stall problem using:
  - Simulation-based hardware information flow tracking
  - A custom-developed, parametrizable Trigger Module
- Validate the methodology on SoC with fully-compliant AXI modules

System-on-Chip – *Typical Architecture*

Controller (AXI Manager)

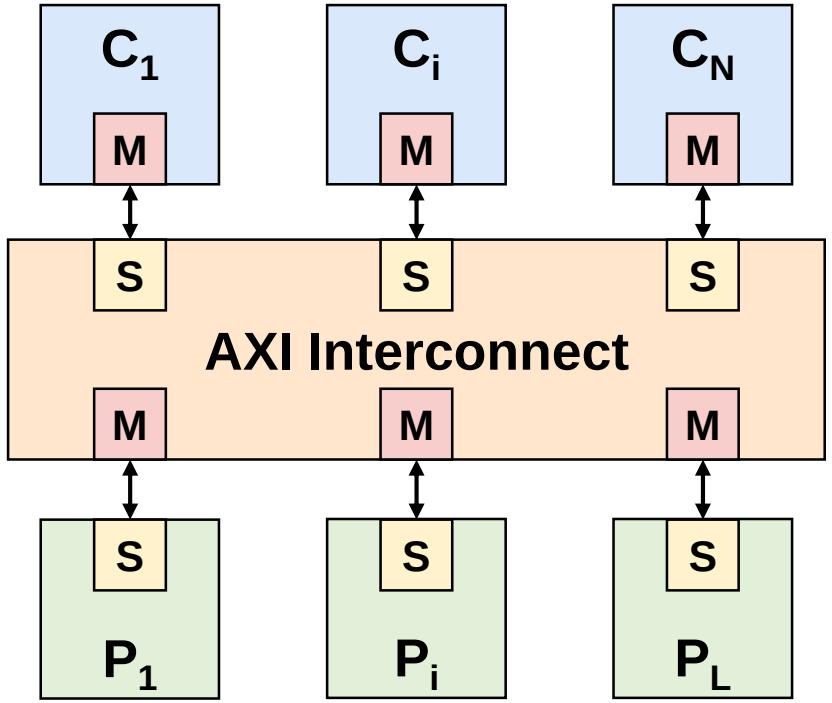
Processors, DMAs, hardware accelerators, etc.

Interconnect (AXI Manager + Subordinate)

Arbitrates access and solves conflicts

Peripheral (AXI Subordinate)

Memories (RAM, ROM, flash, etc.), peripherals, etc.

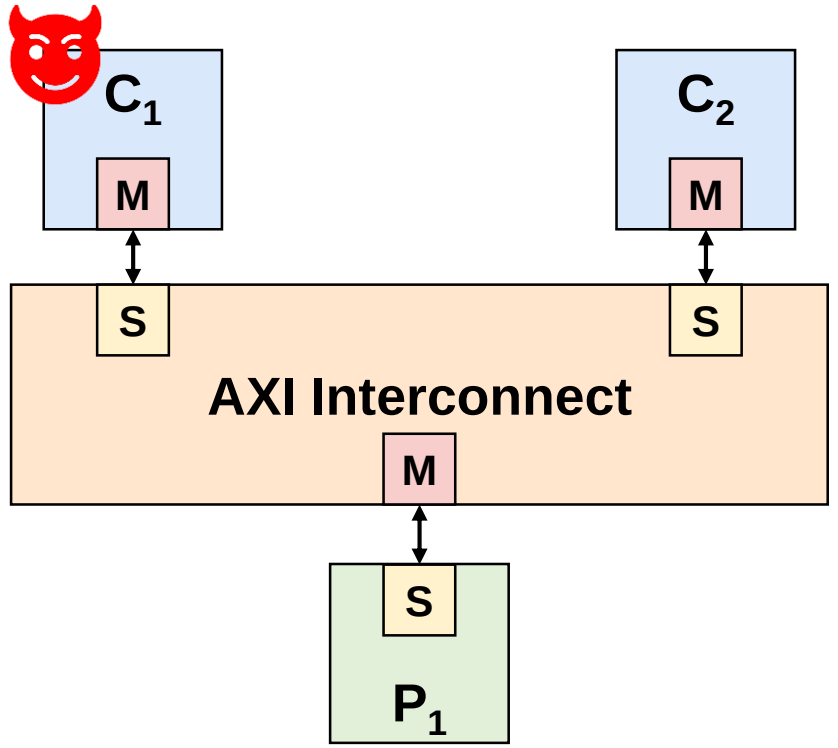


A typical modern SoC architecture (simplified)

Controllers access peripherals via the interconnect

The AXI Bus Stall Problem

T_0	P_1 is idle and ready to fulfill a write request
T_1	C_1 issues write request A_1 directed to P_1
	C_2 issues write request A_2 directed to P_1
T_2	A_1 wins arbitration at I_{AXI} and it is propagated to P_1 by I_{AXI} before A_2
T_3	C_1 delays the data provisioning for A_1 which delays the service of A_2 even if C_2 is ready to provision data for A_2

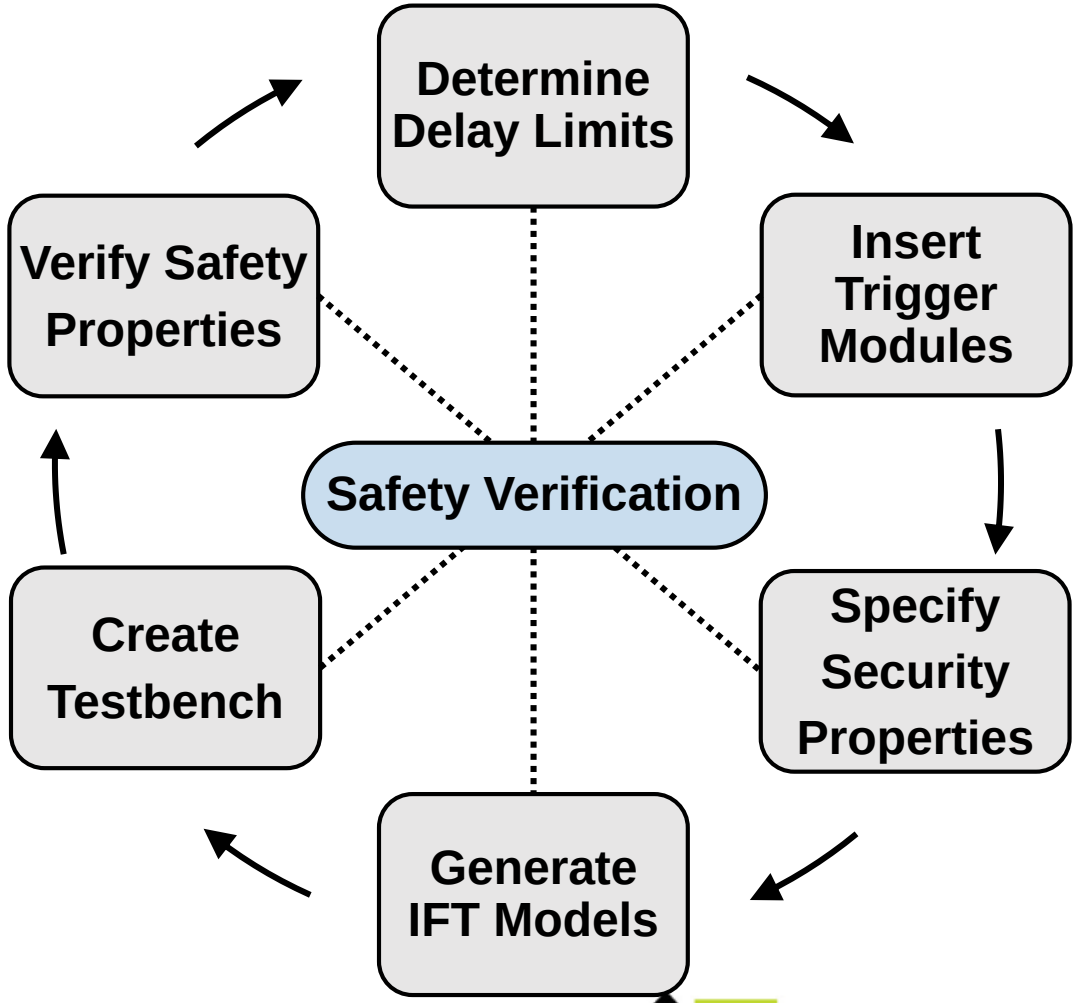


A sampleSoC architecture

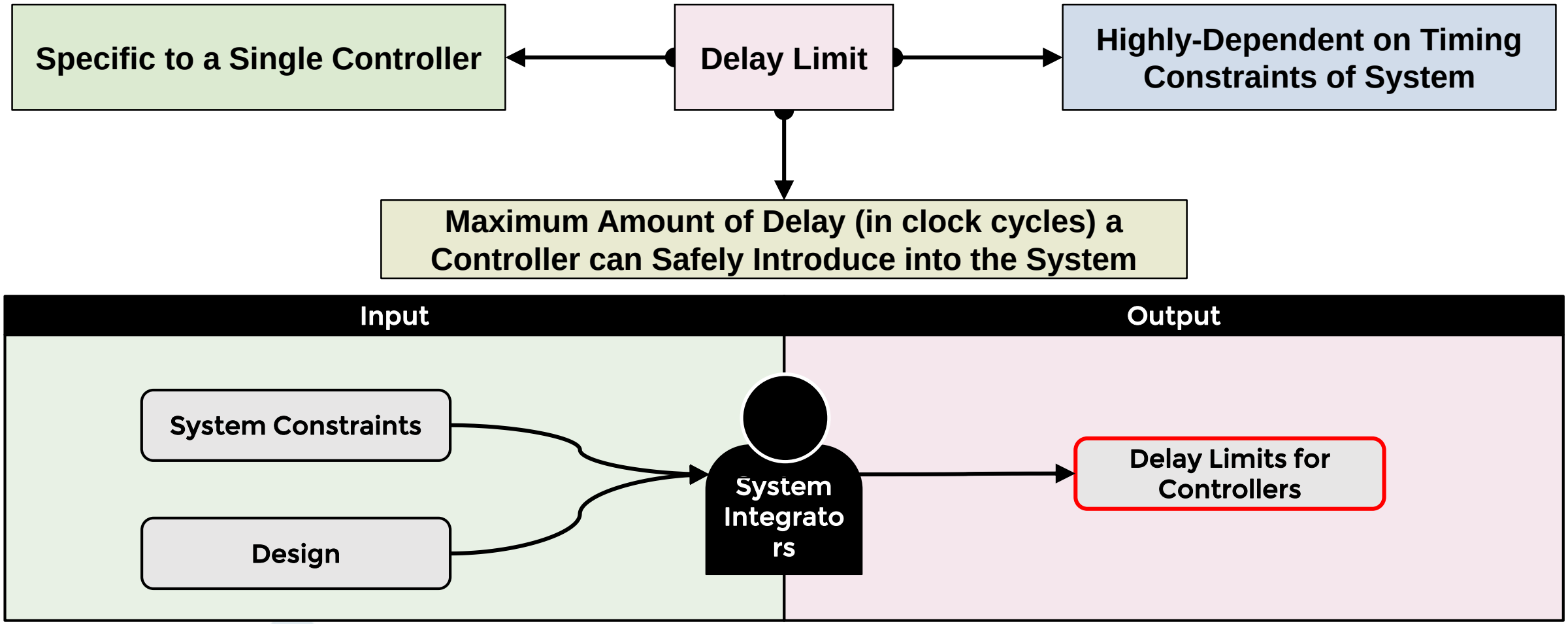
Fully-compliant AXI controllers can delay their data provisioning for an unbounded time

The Safety Verification Flow

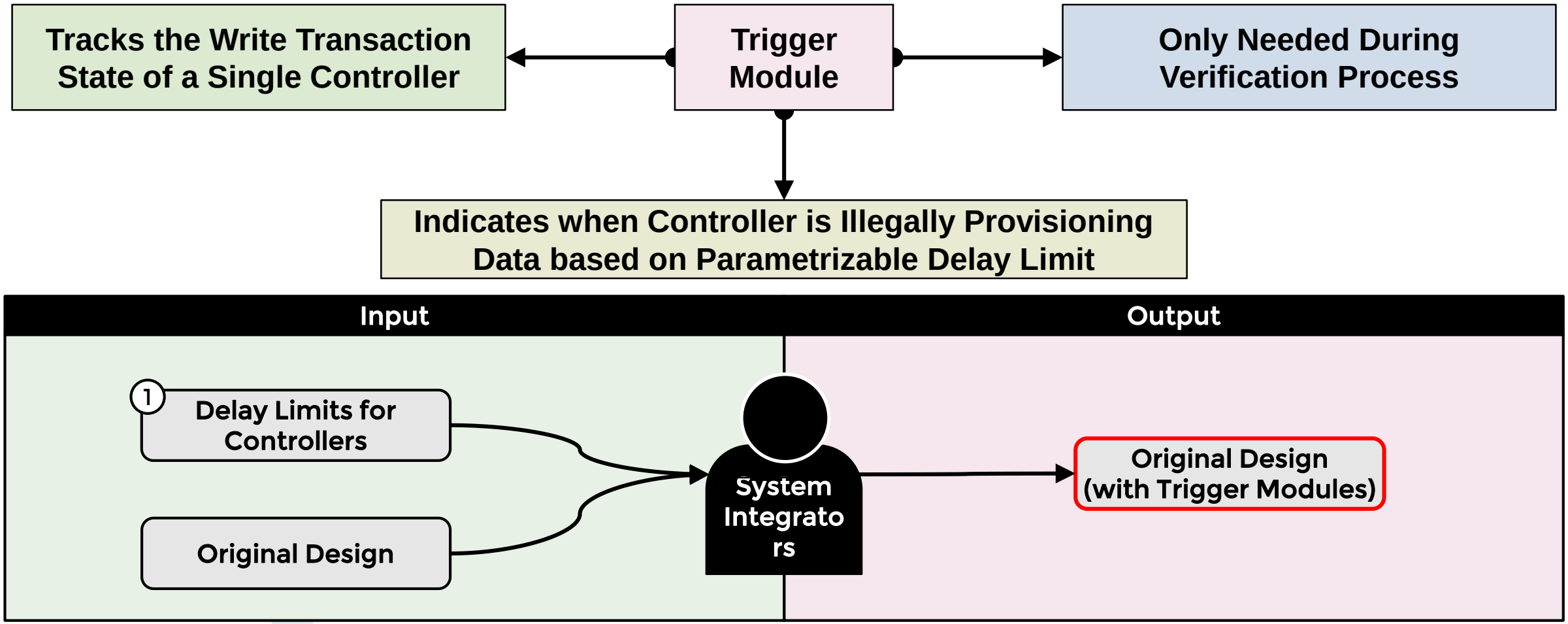
1. Determine the Delay Limits
2. Insert the Trigger Modules
3. Specify the Safety Properties
4. Generate the IFT Models
5. Create a Testbench
6. Verify Properties via Simulation



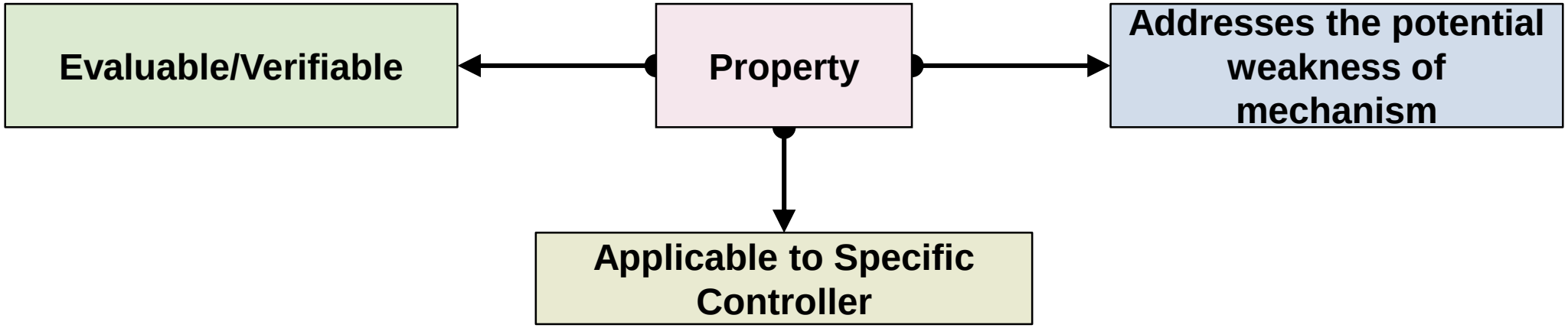
1. Determine the Delay Limits

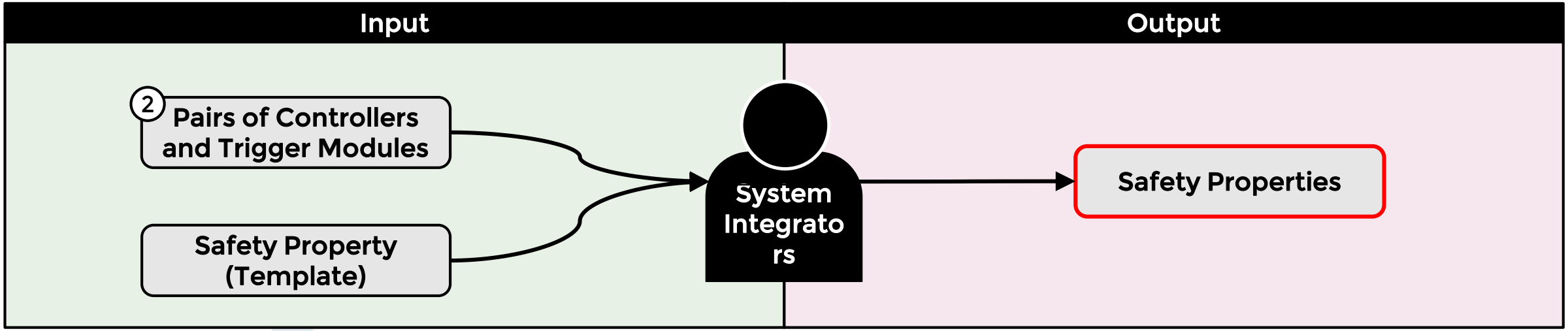


2. Insert the Trigger Modules

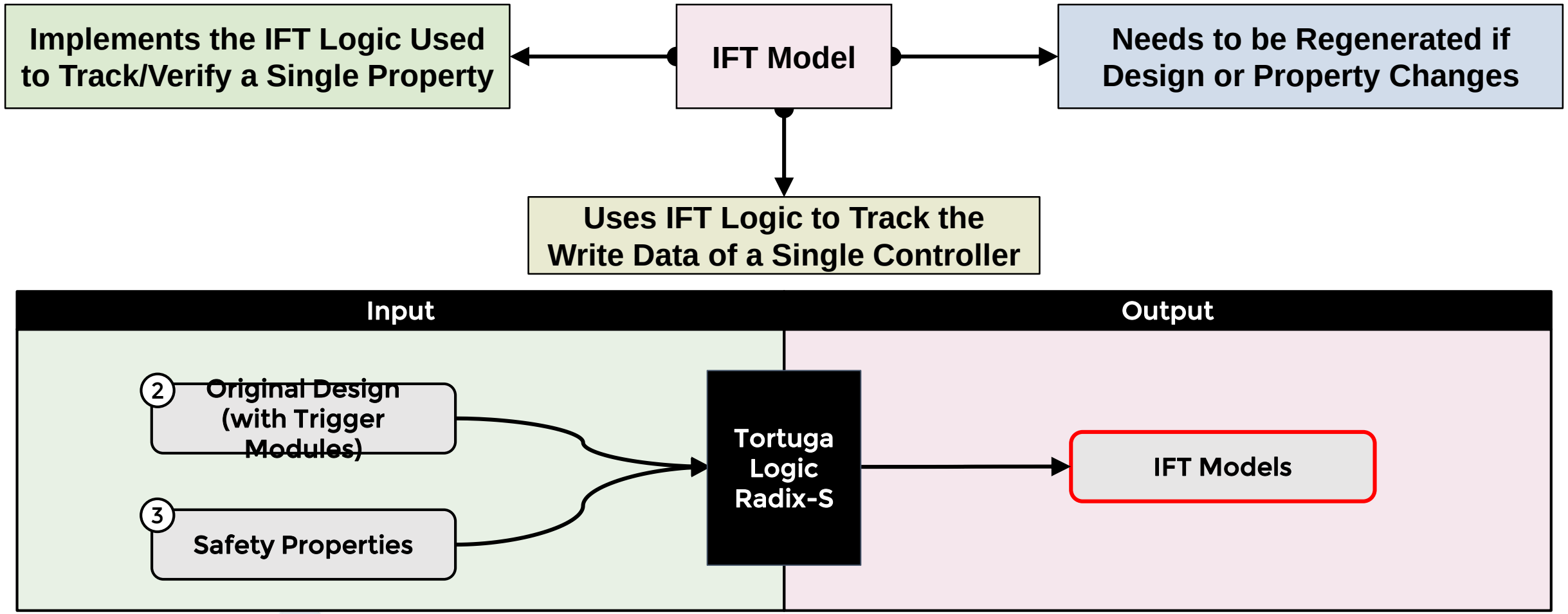


3. Specify the Safety Properties

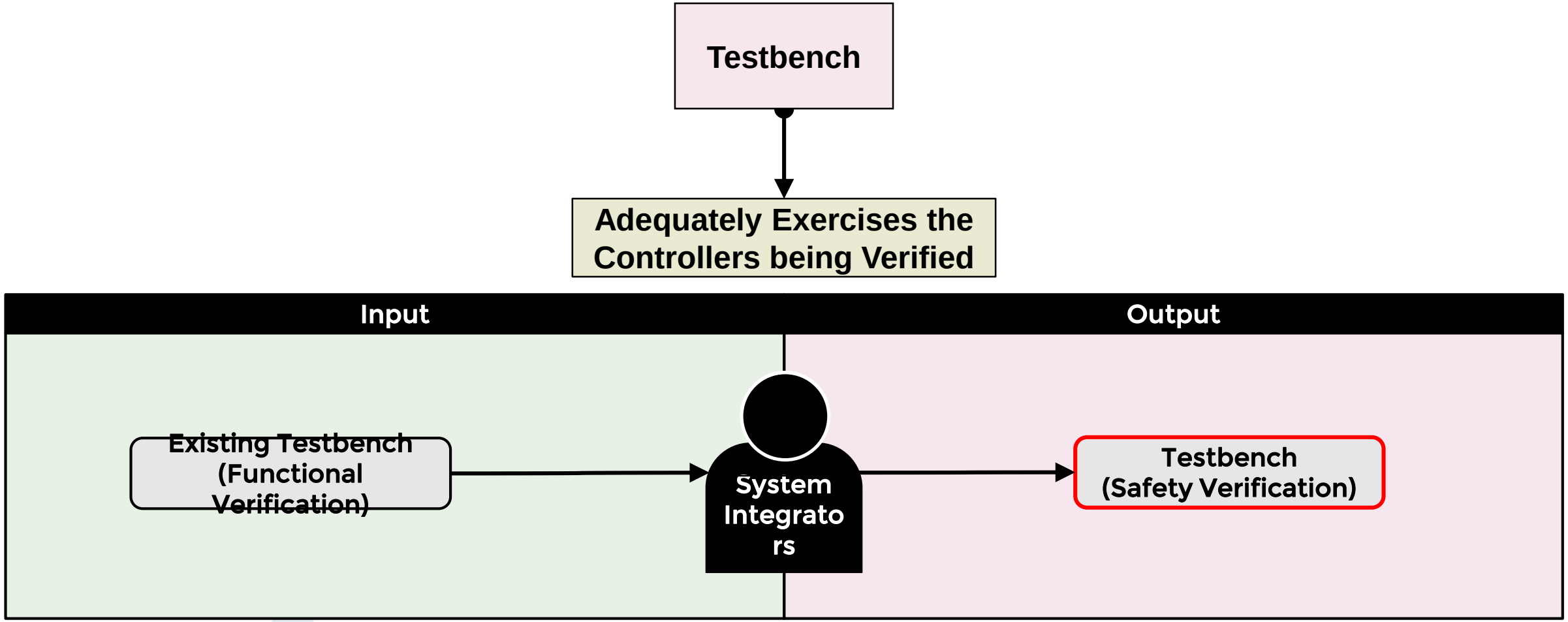




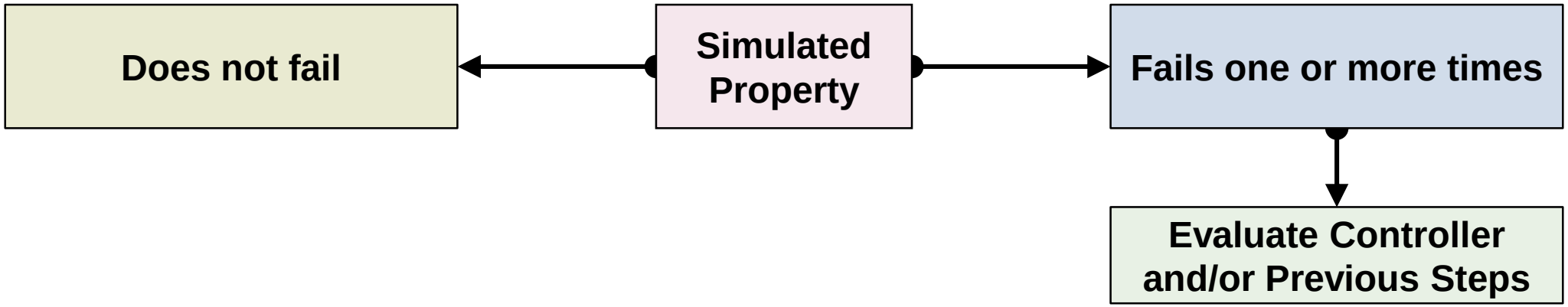
4. Generate the IFT Models

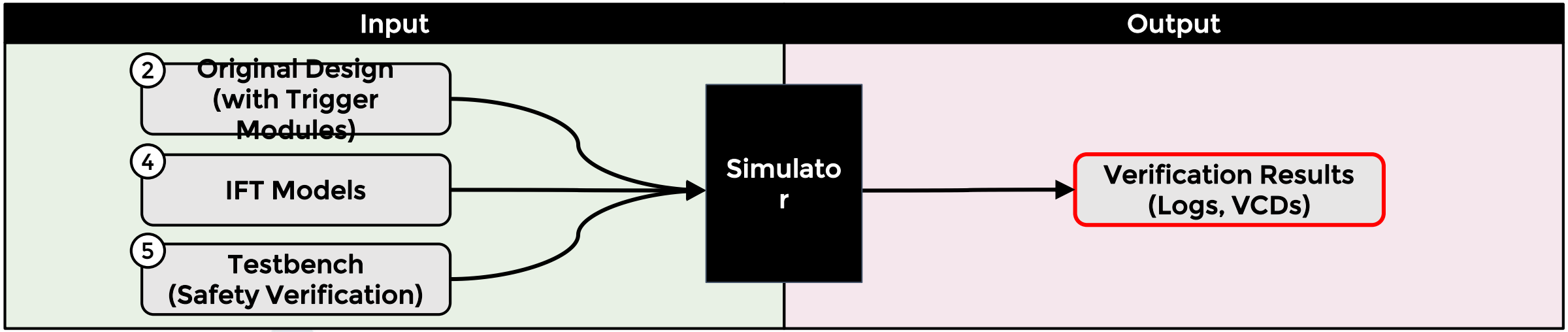


5. Create a Testbench



6. Verify Properties via Simulation





Conclusion

- Introduce the AXI bus stall problem
- Propose a safety verification methodology to identify the AXI bus stall problem using:
  - Simulation-based hardware information flow tracking
  - A custom-developed, parametrizable Trigger Module
- Validate the methodology on SoC with fully-compliant AXI modules
- Future research:
  - Expand the safety verification methodology to address other safety vulnerabilities allowed for by AMBA AXI and other on-chip communication protocols
  - Explore how other verification techniques (e.g., formal methods and standard simulation-based methods) could be used to perform safety verification

Thank You!