AutoSVA: Democratizing Formal Verification of RTL Module Interactions

Marcelo Orenes-Vera, Aninda Manocha, David Wentzlaff and Margaret Martonosi
Department of Computer Science and Electrical Engineering, Princeton University
Princeton, New Jersey, USA
Email: {movera, amanocha, wentzlaf, mrm}@princeton.edu

Abstract—Modern SoC design relies on the ability to separately verify IP blocks relative to their own specifications. Formal verification (FV) using SystemVerilog Assertions (SVA) is an effective method to exhaustively verify blocks at unit-level. Unfortunately, FV has a steep learning curve and requires engineering effort that discourages hardware designers from using it during RTL module development. We propose AutoSVA, a framework to automatically generate FV testbenches that verify liveness and safety of control logic involved in module interactions. We demonstrate AutoSVA’s effectiveness and efficiency on deadlock-critical modules of widely-used open-source hardware projects.

Index Terms—automatic, modular, formal, verification, SVA

I. INTRODUCTION

Heterogeneous SoC design is a lengthy, expensive process that necessitates verification at early stages of development to avoid late bug fixes that thwart performance or area goals [14]. SoC modules may be developed in various contexts and exhibit complicated interactions [2]. With the numerous dependencies that occur between them, module interface verification is necessary to prevent opportunities for livelock and deadlock. Fig. 1 presents the Ariane core [15] and the cache hierarchy of the OpenPiton manycore [1], used as an example throughout the paper. Among the module interactions, the Load-Store Unit (LSU) is critical for the forward progress of the system. For example, a load request to the LSU (blue) must receive a response for a memory request to eventually complete.

Fig. 1. Heterogeneous SoCs such as OpenPiton+Ariane, involve dependencies between modules. Verifying these interactions is critical to guarantee forward progress in the system. For example, a load request to the LSU (blue) must receive a response for a memory request to eventually complete.

Testbenches (FTs) generated by AutoSVA can then be supplied to a FV tool, e.g. JasperGold [5] or the open-source SymbiYosys tool [17]. AutoSVA thereby provides a frontend for automatic FV of an important subset of the correctness problem—a transaction model. This model’s applicability is not limited to modules with explicit requests/responses; it can express other interface mechanisms, e.g. pipeline stages that receive requests from a previous stage and send them to the next stage.

Approach: Given our observations, this work proposes AutoSVA, a framework to automatically generate Formal Verification Testbenches (FT) for a given DUT. The designer of the DUT only needs to identify relevant transactions and annotate them in the module interface using a simple language. The framework then generates properties that verify the transactions are well-formed and make forward-progress: they satisfy liveness (every request is eventually followed by a response) and safety (expectations for attributes of the response). Through its automated reasoning, AutoSVA creates the necessary scaffolding code to express these properties and tool-specific commands to drive the FV process, alleviating the hardware designer from significant engineering effort and democratizing the use of FV for verifying forward progress.

Our main contributions are:

- A language that creates a unified transaction abstraction to denote RTL interface interactions and dependencies. This enables automatic reasoning about RTL properties.
- An automated procedure to generate FTs that express liveness properties about transaction temporal dependencies and safety properties about control-logic attributes.
- Demonstration of AutoSVA’s effectiveness on 7 control-


```verilog
reg [TRANS_WIDTH-1:0] lsu_load_transid_sampled;
wire lsu_reg_hsk = lsu_reg_val && lsu_reg_rdy;
wire lsu_load_set = lsu_reg_hsk & & lsu_reg_transid == symb_lsu_transid;
wire lsu_response = lsu_res_val & & lsu_res_transid == symb_lsu_transid
always_ff @posedge clk || negedge rst_ni begin
  if (rst_ni) // counting transaction
    lsu_load_sampled <= '0;
  else if (lsu_load_set || lsu_load_response)
    lsu_load_sampled <= lsu_load_sampled + 1;
end end

co__lsu_request_happens:: cover (property (lsu_load_sampled > 0);
  // Assume that a transaction is stable until acknowledged
  am__lsu_load_stability:: assume (property (lsu_reg_val && lsu_reg_rdy ==
    $stable([lsu_reg_stable]));
  // Assert that if a valid transaction eventually is ack'ed or dropped
  as__lsu_load_hsk_or_drop:: assert (property (lsu_reg_val ||
    s_eventually([lsu_reg_hsk || lsu_reg_rdy]));
  //Assert that every request has response, and every response had a request
  as__lsu_load_eventual_response:: assert (property (lsu_reg_set ||
    s_eventually([lsu_load_response]));
  as__lsu_load_had_a_request:: assert (property (lsu_load_response ||
    lsu_load_set || lsu_load_sampled > 0);
```

Fig. 2. To verify the load interface of the LSU, a hardware designer
would need to write many SVA properties and auxiliary code. AutoSVA
automatically generates all modeling, removing the burden from the designer.

Critical RTL modules of the widely-used open-source projects Ariane and OpenPiton [1], [13]. As one example, within 1 hour, AutoSVA generated a FT for Ariane’s MMU, discovered a bug, and verified the bug-fix.

II. MOTIVATING EXAMPLE

SVA is SystemVerilog’s formal specification language [10], and offers a mature approach for verifying RTL. It can express Linear Temporal Logic (LTL) formulas over interface signals to build properties about module interactions. LTL specifies temporal relations, which fall into two major classes: safety and liveness properties. Safety properties specify that “nothing bad will happen”, e.g. a response must have had a request; while liveness specify that “something good will happen”, e.g. a request is eventually acknowledged.

Fig. 2 presents a subset of the modeling and properties that are necessary to verify forward progress for the load-store unit (LSU) in Ariane (depicted in Fig. 3). For example, `lsu_load_eventual_response` is a liveness property to check that any load request eventually receives a response with the same transaction ID. Verifying expectations about module interfaces goes beyond writing properties; it requires code to sample transactions and symbolic variables to track them. AutoSVA automatically generates all of this necessary code.

Properties in SVA can use one of three directives: `assert`, `assume` and `cover`. Assumptions have different meanings based on how input stimuli are generated. In RTL simulation, inputs are driven either by manual or random tests, and thus `assume` has the same meaning as `assert`. i.e. they check that the property holds. Conversely, FV tools treat inputs as Boolean variables, and assumptions constrain the state space exploration by preventing some behaviors, while `assertions` check that properties hold on the explored paths. FV tools then use a variety of solver engines [6] based on formal methods, such as model checking, which uses SAT (satisfiability) [3] or BDD (binary decision diagrams) [12], to exhaustively search for property violations. FV search may result in a counterexample (CEX) that highlights the violation of a property, or proof that properties hold, i.e. the solver converges and finds no CEXs.

The underlying dynamics of FV and SVA make it difficult to intuitively understand the consequences of various properties expressed, such as the behavior of symbolic variables, e.g. `symb_lsu_transid` in Fig. 2 which allow the tracking of indices with a single assertion. Furthermore, subtle mistakes in assumptions, e.g. using the `|->` implication symbol in the `lsu_stability` assumption, can over-constrain the state space and end up proving vacuity. Manually inserting assertions can be cumbersome and error-prone for a hardware designer, and particularly frustrating when CEXs appear due to illegal inputs of not yet modeled interfaces [8]. Thus, AutoSVA automatically models and expresses the expected behavior for module transactions.

Hardware designers can employ SVA properties for Test-Driven-Development (TDD), where CEXs help to refine the design [16]. Moreover, this can be applied at early stages of RTL module development by using unit-level FV [4]. However, FV’s steep learning curve and necessary engineering effort preclude designers from using it in practice [15].

AutoSVA democratizes FV for hardware designers and makes TDD practical by automating a key component of the FV problem: liveness and safety of module interfaces. Instead of aiming to support functional FV, which is very implementation-dependent, AutoSVA focuses on verifying that modules interact through well-formed transactions. This verification entails checking certain attributes over the control logic involved in transactions and mapping them to properties that ensure that every module makes progress (does not hang).

Fig. 3 presents an example of the simple usage of AutoSVA’s language. These annotations unleash automated reasoning to generate the modeling and properties (shown in Fig. 2) surrounding liveness and safety for the Ariane core’s LSU. Section III explains the syntax of the AutoSVA language and semantics of each annotation. Section IV shows how these annotations can be applied to different interface styles.

III. THE AUTOSVA FRAMEWORK

AutoSVA focuses on verifying liveness, and its well-formed transactions allow it to utilize a common abstraction from RTL interfaces that avoids the complexity of specific module implementations. By capturing a common design-pattern, AutoSVA can automatically generate useful Formal Testbenches (FT). We denote a FT as `useful` when it (1) has sufficient mod-
ule interface modeling to avoid spurious CEXs and capture relevant CEXs which lead to uncovering bugs, and (2) does not miss legal scenarios due to over-constraining assumptions. Moreover, AutoSVA reduces the state-explosion scalability problem because it deliberately focuses on control logic and FV tools can be instructed to automatically ignore datapaths.

Fig. 4 presents an overview of AutoSVA’s verification process. AutoSVA takes as input the interface declaration section of the RTL module acting as the DUT. The interfaces should be annotated using AutoSVA’s language for interface abstraction (defined at Section II-A). Once the abstraction is defined for a DUT, AutoSVA generates the FT that includes a property file describing the properties to verify, all necessary modeling annotations, which is especially useful for early-stage RTL design. If they follow the ATTRIB relation, AutoSVA can automatically identify these fields without prefixed with an interface name.

A. AutoSVA Language to Express Transactions

AutoSVA’s transaction abstraction involves two events connected with an implication relation. From the DUT’s perspective there are two types of transactions: (1) incoming transactions describe when a DUT receives a request and is responsible for eventually triggering a well-formed response or another request, and (2) outgoing transactions describe when a DUT triggers a request that eventually must receive a response.

The two events in a transaction are associated with RTL interfaces, which are the connection points of RTL modules. For example, incoming transactions can map a cache lookup interface to define a liveness condition that the cache lookup should eventually have a response, and to define a safety condition that this response must satisfy certain properties, e.g. maintain the same transaction ID the request had.

AutoSVA maps transaction events to interfaces through annotations expressed in its language. These language annotations are written as Verilog comments on the interface declaration section of an RTL file to identify module interfaces that participate in transactions. To distinguish these annotations from regular code comments, AutoSVA requires annotations to be preceded with an AUTOSVA macro, or be contained within a multi-line comment region that starts with it.

Table I presents the formalization of the AutoSVA language. Each column represents an interface attribute. If an attribute is defined on an interface, then an attribute relation must be prefixed with the interface name.

Table II presents the formalization of the AutoSVA language. Each column represents a property generated for each transaction attribute.
the two interfaces communicate and thus a liveness property is generated for the transaction. The absence of an ack signal indicates the request/response is always accepted.

Some of the properties expressed in Table II cannot be expressed in SVA directly, and thus AutoSVA generates all necessary auxiliary Verilog code. For example, verifying that every response followed a previous request requires counting the number of ongoing transactions (done with registers in Fig 3). The transid attribute allows tracking transactions to reason about other attributes, such as data, which is used to verify data integrity. This is important for interface fields which are immutable between P and Q, e.g. data in a queue or address in a memory request.

Attributes marked with * at Table II generate properties that are asserted when the transaction is incoming and assumed when outgoing. E.g., for the val attribute, the word “eventually” indicates liveness when the DUT is expected to respond and fairness when it is waiting for a response. For attributes stable and transid_unique, the opposite holds; properties are assumed on incoming and asserted on outgoing transactions. The attribute active is always asserted when defined.

Submodule Properties: When the DUT has a submodule whose inputs are driven by actual logic, it is worthwhile to ensure that assumptions about these inputs hold. AutoSVA assumptions can be converted into assertions by changing the value of the ASSERT_INPUTS parameter. Submodule properties can be linked to the parent’s through AutoSVA’s parameters: "-AM" includes the properties when the submodule was the DUT (assumptions over outgoing requests) and "-AS" converts all assumptions into assertions.

End-to-End Properties: SVA allows writing properties that use internal RTL logic (not visible at the interface). While this is often necessary for full functional verification, it causes properties to depend on RTL implementation details. To overcome this, AutoSVA writes end-to-end properties which solely describe interface signals, but cover the whole path from input to output interface. End-to-end properties are implementation-agnostic, and thus can be automatically generated pre-RTL, making AutoSVA a great framework for Test-Driven-Development (TDD).

Property Reuse: In addition to FV, AutoSVA property files can be utilized in a simulation testbench to ensure that assumptions hold during system-level testing. Although many RTL simulation tools do not support liveness properties, all control-safety properties and X-propagation assertions can be checked during simulation. AutoSVA generates X-propagation assertions, which check that when the val signal of an interface is asserted, none of the other attributes have value X (concurrently 0 and 1). Because formal tools do not consider X’s and instead assign arbitrary values of 0 or 1, these assertions are only checked during simulation (under a XPROP macro).

C. AutoSVA Implementation and Process Steps

AutoSVA is implemented in Python using only standard libraries to provide portability and ease of use. AutoSVA generates FTs in under a second. Fig. 5 details its five steps.

![Fig. 5. Steps of the AutoSVA framework. It receives an annotated RTL file and the FV tool to target, and it outputs a FT that is ready to be run.](image)

1) Parser: AutoSVA parses the signal declaration section of the annotated RTL file to identify global parameters, e.g. cache associativity or queue size, annotations in the AutoSVA language, and interface input/output signals. Based on the annotations, the parser identifies which pairs of interfaces participate in transactions and creates a mapping from interface pairs (P and Q) to a list of their attribute definitions.

2) Transaction Builder: AutoSVA builds transaction objects based on interface fields and implication relations identified by the parser. During this process, AutoSVA can detect syntax errors in annotations, e.g. when transid or data fields are defined in only one of the interfaces of a transaction, or with mismatched data widths.

3) Signal Generator: Before generating properties based on transactions, AutoSVA generates auxiliary signals, such as symbolics, which are unassigned variables used to build assertions. Symbolic variables are unconstrained, and allow FV tools to explore all their possible values in a single assertion. For example, a single assertion can be used to reason about all lines of a cache if a symbolic signal is used to index the cacheline. AutoSVA also generates handshake signals (as conjunctions of val and ack) to indicate that a request or response takes place.

4) Property Generator: AutoSVA creates properties based on the transaction attributes and type (incoming or outgoing). These properties can verify liveness, uniqueness, data integrity, stability, or X-propagation (detailed in Section III-B). SVA properties are explicitly written in the property file. AutoSVA does not use SVA macros or checkers to provide better readability in case the user wants to explore the properties or a verification engineer wants to extend the FT for functional correctness. The properties are tool-agnostic, and written to be most efficient for FV tools to run, e.g. using symbolic indexes for transid tracking. The authors have created this tool based on lessons learnt from prior art [7], [8], [15] and years of industry and academic experience with FV of RTL.

5) FV Tool Setup: Once the SVA properties are generated, AutoSVA links them to the FV tool that the hardware designer selects. Furthermore, AutoSVA supports linking the FTs of submodules of the DUT, that had already been generated, by using script parameters during AutoSVA’s invocation.
IV. EVALUATING THE AUTOJAVA FRAMEWORK

We utilize multiple metrics to evaluate AutoJAVA: (1) its ability to find bugs, both known (open issues) and new bugs; (2) the speed of bug discovery, based on tool runtime and test length; (3) amount of engineering effort, measured in time spent writing the transaction annotations; and (4) bug-fix confidence, whether the bug-fix leads to a proof or new CEX.

We study these metrics in mature, taped-out, open-source hardware projects: 64-bit RISC-V Ariane Core [18] and the OpenPiton manycore framework [1]. We have selected 7 RTL modules that are critical for forward-progress and thus require exhaustive testing. Table I lists these modules as well as the outcome of formally verifying them using testbenches generated by AutoJAVA. These outcomes consist of proofs and models to verify forward progress. We also demonstrate AutoJAVA for early-stage verification by applying it to a new unit, Mem Engine, which connects to OpenPiton’s NoC by reusing its encode/decode buffers.

AutoJAVA supports several FV tools, so we elect to perform evaluations using JasperGold 2015.12. Additionally, to check that AutoJAVA properties are compatible with system-level simulation, we bind the property files to the in-place testbench using VCS-MX 2018.09.

Applying the AutoJAVA language to RTL modules: A key component of AutoJAVA is its transaction abstraction that is broad enough to apply to most RTL interface styles and specific enough to generate useful properties. Fig. 7 presents a few examples of how AutoJAVA can be applied to a wide range of interfaces based on common possible scenarios.

Single Ongoing Transaction: When there is only one ongoing transaction in a module, it can be modeled simply by not defining the transid attribute, which is the case for the ptw_dcache and dtlb_ptw transactions in Fig. 7. This principle works for both incoming and outgoing transactions.

Multiple Outstanding Transactions: When transactions can be in-flight simultaneously, it can be modeled by annotating the tracking field with transid, e.g., mshrid for mem-engine_noc. Tracking requests allows AutoJAVA reasoning about integrity of transid and data fields. If requests are not tracked, AutoJAVA still checks that there are no more responses than requests and that every transaction eventually finishes.

No Ack signal: When an interface does not have an ack signal but the module cannot always accept new requests, AutoJAVA allows defining ack by reasoning about other signals. In the case of dtlb_ptw, the ack field is defined based on the active signal, that indicates when the PTW is busy. Defining stable alongside ack means that AutoJAVA will model the payload to remain stable until the request is ack’ed.

Results: Table III presents the 7 Ariane and OpenPiton modules that were tested using FTs. AutoJAVA generated a total of 236 unique properties based on 110 LoC of annotations.

First, FTs of Ariane’s PTW and TLB resulted in 100% of the properties being proven at unit-level after 30 minutes of human effort to define the correct transactions. Next, the MMU FT was set up after 10 minutes of adding a new transaction and reusing the properties of its submodules’ FTs. These results demonstrate that AutoJAVA is quick to use and effective at verifying forward progress in control-critical modules.

Fig. 6 shows the hierarchy of the Ariane modules we have tested. The MMU FT (blue) checks that every request from the LSU eventually receives a response, and that no response occurs without a prior request. Before it uncovered a real bug, AutoJAVA found an interesting CEX: an ITLB miss was never filled because the PTW was always busy with DTLB misses, i.e., DTLB has static priority over ITLB. This fairness problem cannot happen in practice since one instruction cannot do many DTLB lookups. Since the trace was quick (<1s) and short (<4 cycles), it was straightforward to identify the cause of the CEX and add an assumption to remove it.

---

| RTL Module | Result |
|------------|--------|
| A1. Page Table Walker (PTW) | 100% liveness/safety properties proof |
| A2. Trans. Look. Buffer (TLB) | 100% liveness/safety properties proof |
| A3. Memory Mgmt. Unit (MMU) | Bug found and fixed -> 100% proof |
| A4. Load Store Unit (LSU) | Hit known bug (issue #538) |
| A5. L1-LS (write-back) | Hit known bug (issue #474) |
| O1. NoC Buffer | Bug found and fixed -> 100% proof |
| O2. L1.5$ (private) | NoC Buffer proof, other CEXs |
Bug1. Ghost Response on MMU: The next CEX uncovered a bug that was triggered when the MMU receives a misaligned request from the LSU. The MMU responds immediately with a bad alignment response, but the DTLB still misses and the PTW is activated (bad behavior). In the case of a page fault, the MMU generates a second “ghost” response to the LSU, raising an exception. This bug was found by the FV tool in less than a second, producing a 5-cycle trace that allowed us to quickly identify the problem and produce a bug-fix (masking the PTW request with the misaligned signal) with high confidence, as the formal tool found a proof in a few seconds for the previously failing assertion. In 5 minutes, the MMU FT proof-rate was 100%. The Ariane maintainers confirmed the bug and the fix.

Hitting Known Bugs: The LSU FT hit (in 1 second) a bug that was recently discovered on a long FPGA run: an ongoing load hits an exception caused by a later load. The Ariane maintainers welcomed a FT where they could validate that the bug-fix solves the problem and does not break anything else. Similarly, the L1-I$ FT was able to hit a reported bug.

Bug2. Deadlock in NoC Buffer: AutoSV A found a deadlock bug in an underdeveloped part of Mem Engine that connects to the OpenPiton NoC. Since the interfaces mostly matched the AutoSV A language, the FT was generated with just 3 lines of code (shown in mem-engine_noc at Fig. [7]). The first CEX to the liveness assertion revealed a bug that arises from the reuse of the NoC buffer from the L1.5$ for Mem Engine. The buffer assumes that the input does not drive more requests than the number of buffer entries, which is violated in Mem Engine. After fixing the bug (adding a “not-full” condition to the ack signal), the formal tool resulted in a proof.

Lastly, the FT of OpenPiton’s L1.5$ showed that the condition added to the NoC buffer did not break the properties for its buffer instance. Other properties, e.g. that every cache miss is eventually filled, showed CEXs due to under-constraints in the message types. AutoSV A provides the FT foundation that the L1.5$ designer can refine with assumptions to remove spurious CEXs. The testbench can also be extended with more assertions to achieve complete functional verification.

V. RELATED WORK

Early works focused on developing methods for formal verification of RTL correctness [4]. These include model checking, which relies on SAT solvers or BDDs, and Assertion-Based Verification (ABV), which builds on top of model checking to verify control logic, design interfaces, and data integrity. The emergence of SVA [10] popularized ABV for verification engineers [15]. More recent work focuses on generating SVA from a higher level language [9]. [11]: RTLCheck verifies RTL pipeline implementations against their memory consistency model (MCM) axiomatic specifications; ILA generates a Verilog model of the design from the ILAEng functional specification, and compares it against the RTL implementation [9]. Although these methods automatically generate SVA, defining high-level models and matching them to RTL signals still require significant effort and knowledge, which may discourage hardware designers from using them.

VI. CONCLUSION

This work presents AutoSV A, a tool to automatically generate testbenches for unit-level FV. Based on annotations made in the signal declaration section of an RTL module, AutoSV A generates liveness and safety properties about control logic to verify forward-progress. Thus, hardware designers can verify their designs at unit-level without requiring FV expertise and with the minimal effort of writing RTL module interface annotations. This pays off quickly, as performing FV early can save significant debugging time during system-level simulation and increase designer confidence that the system will not hang.

We have shown that AutoSV A is useful and effective with an evaluation on widely used open-source hardware projects. This discovered bugs and provided proofs of 7 control-critical RTL modules. AutoSV A generated a total of 236 unique properties (no loops) based on 110 LoC of annotations. The generated FTs are extensible and so they are included in the open-source repository of this work. We envision AutoSV A to become a standard language to define RTL modules’ interface expectations, eventually integrated into the SVA specification.

REFERENCES

[1] J. Balkind, K. Lim, F. Gao, J. Tu, D. Wentzlaff, M. Schaffner, F. Zaruba, and L. Benini, “OpenPiton+ Ariane: The first open-source, SMP Linux-booting RISC-V system scaling from one to many cores,” in Computer Architecture Research with RISC-V, CARRV, vol. 19, 2019.
[2] J. Balkind, K. Lim, M. Schaffner, F. Gao, G. Chirkov, A. Li, A. Lavrov, T. M. Nguyen, Y. Fu, F. Zaruba et al., “BYOC: a ‘bring your own core’ framework for heterogeneous-ISA,” in ASPL’25, 2020, pp. 699–714.
[3] A. Biere, A. Cimatti, E. Clarke, and Y. Zhu, “Symbolic model checking without BDDs;,” in International conference on tools and algorithms for the construction and analysis of systems. Springer, 1999, pp. 193–207.
[4] J. Buckingham, “Formal for designers,” in Agile Test Driven Development forASIC, 2016.
[5] I. Cadence Design Systems, “Jaspergold apps user’s guide,” 2015.
[6] ——, “Jaspergold engine selection guide,” 2016.
[7] E. Cerny, S. Dudani, J. Havlicek, D. Korchenny et al., SVA: the power of assertions in SystemVerilog. Springer, 2015.
[8] C. Cumming, “SystemVerilog Assertions - best known practices for simple SVA usage,” SNUG Silicon Valley, 2016.
[9] F. Zaruba and L. Benini, “64-Bit RISC-V 6-stage Ariane core (CVA6),” https://github.com/PrincetonUniversity/AutoSV A.
[10] IEEE Standard for SystemVerilog—Unified Hardware Design, Specification, and Verification Language, IEEE 1800-2012 Std., 2013.
[11] Y. A. Maneker, D. Lustig, M. Marconosi, and M. Pellauer, “RTLCheck: Verifying the memory consistency of RTL designs,” in 2017 50th Annual IEEE/ACM MICRO, 2017, pp. 463–476.
[12] K. L. McMillan, “Symbolic model checking,” in Symbolic Model Checking. Springer, 1993, pp. 25–60.
[13] Ping Yeung and K. Larsen, “Practical assertion-based formal verification for SoC,” in 2005 Intl. Symposium on System-on-Chip, 2005, pp. 58–61.
[14] A. Reid, R. Chen, A. Deligiannis, D. Gilday, D. Hoyes, W. Keen, A. Pathirane, O. Shepherd, P. Vrabel, and A. Zaidi, “Instruction-level abstraction (ILA): A uniform specification for system-on-chip verification,” ACM Transactions on Design Automation of Electronic Systems (TODAES), vol. 24, no. 1, pp. 1–24, 2018.
[15] E. Seligman, T. Schubert, and M. A. K. Kumar, Formal verification: an introduction, 2nd ed. Springer, 2009.
[16] S. Sutherland, “What put assertions in my RTL code? And why? How RTL design engineers can benefit from the use of SystemVerilog Assertions,” SNUG Silicon Valley, pp. 1–6, 2015.
[17] C. Wolf, “SymbiYosys,” https://github.com/YosysHQ/SymbiYosys.
[18] F. Zaruba and L. Benini, “64-Bit RISC-V 6-stage Ariane core (CVA6),” https://github.com/openhwgroup/cva6.