Formal signoff for Cross-Module Design logic: A novel approach to manage formal scope in increasingly complex systems

Sakthivel Ramaiah, Design Engineering Architect
Sai Asrith Tabdil, Design Engineer II
Sorna Inian, Sr Application Engineer
Clarice Ferreira Oliveira, Lead Application Engineer

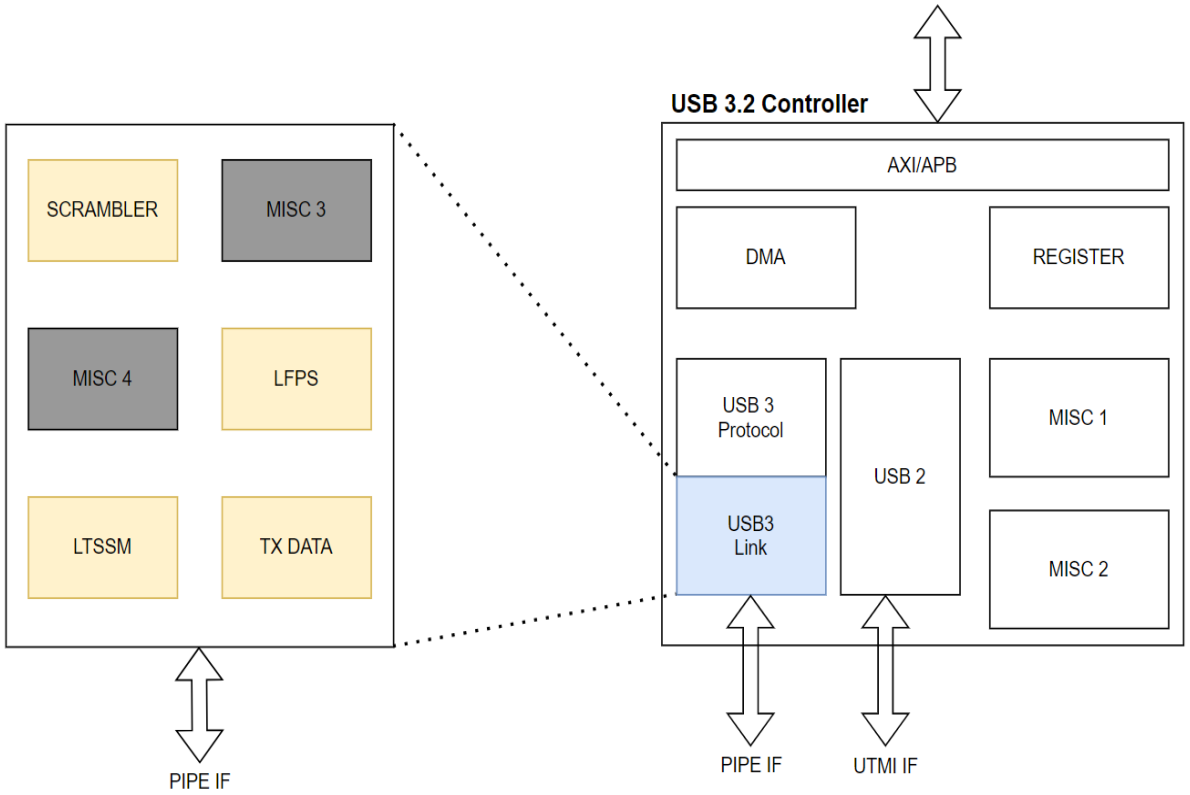
cadence

SPONSORED BY CEDA IEEE Council on Electronic Design Automation sigda acm

Motivation

- As systems become more complex, verifying cross-module logic posses significant challenges for formal verification due to state space explosion and unclear assertion boundaries.
- To mitigate last stage bugs, many designs include chicken bits to disable potential risky features, which highlights the lack of confidence in current verification coverage.
- This paper proposes an approach to manage formal scope across modules more effectively, aiming to reduce verification gaps, improve modularity, and build trust in formal sign off for complex systems.

Introduction

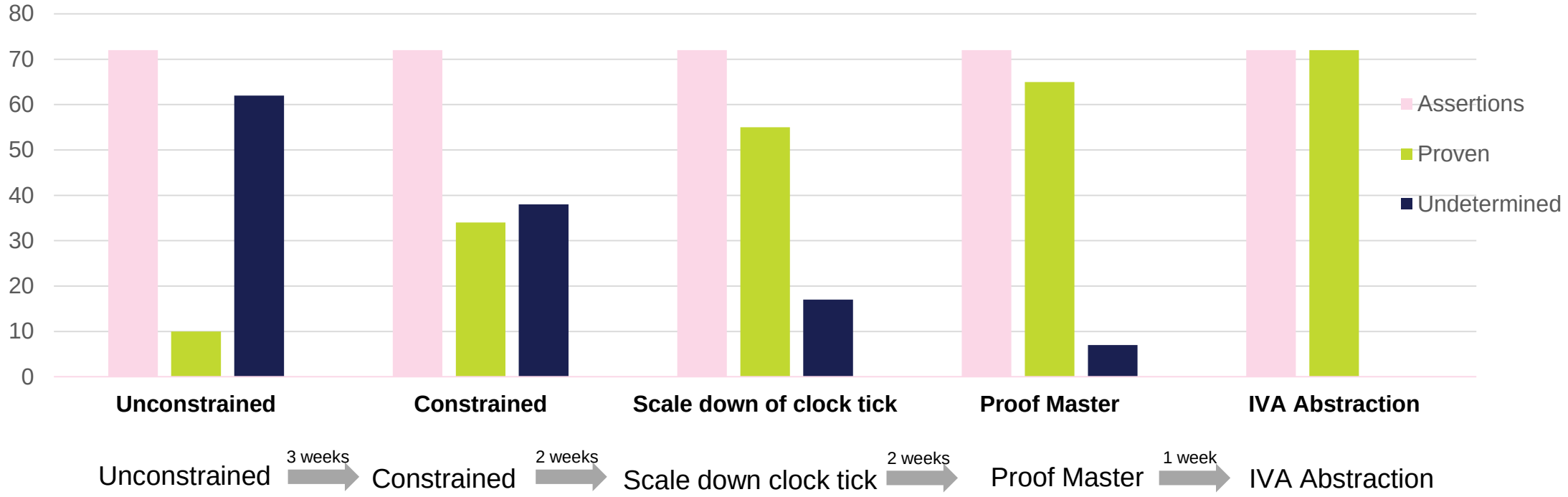


USB3.2 Controller IP and USB3 LINK module

- The feature discussed in this presentation is Compliance mode of USB 3.2 Controller.
- The link layer consists of multiple submodules but the Feature Under Verification (FUV) logic is spread across LTSSM, Scrambler, LFPS and TX Data as shown in the diagram.
- The link layer is taken as the DUT and black boxing is applied for the miscellaneous blocks which are not related to the feature.
- Compliance is one of the states of LTSSM and it consists of 16 patterns which also includes the rate change from GEN1 to GEN2.

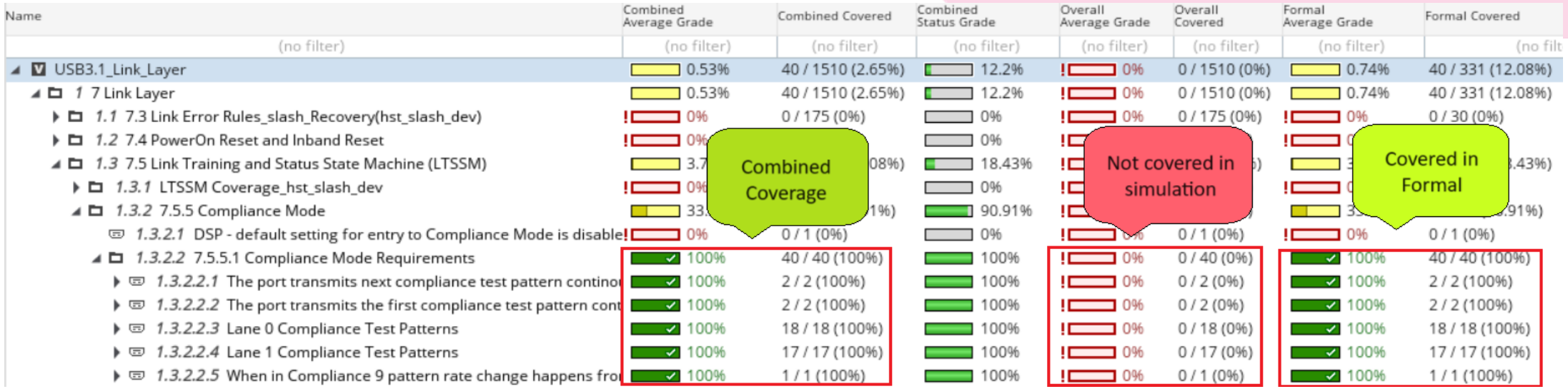
Technique	Purpose and Benefits
Scale down the clock ticks/timers	• To reduce the complexity and run time we scaled down the clock ticks used. • This has allowed the formal tool to converge quickly.
Black boxing and cut points	• Black boxing irrelevant logic to the feature. • This allows the tool to reach more sequential depth. • This reduces the state space and reduces the proof time.
Constraints	• Constraints help in reaching the intended feature quickly narrowing the state space of verification.
Proof Master(AI/ML based feature)	• Proof Master uses ML algorithm to allocate suitable engines dynamically based on the previous run. (Proof Orchestration) • It uses historical knowledge to better use the computational resources. (proof caching and PPD) • With the help of previous run, tool engines effectively work on undetermined assertions and help in converging them.
Abstraction Technique	• Initial Value Abstraction abstracts away the specific initial values of registers, reducing the state space. • By eliminating the need to specify initial values, IVA enables faster convergence of formal proofs.

Results



- The graph shows the number of undetermined properties present for a run time of 24 hours.
- Using Initial Value Abstraction method, 7 undetermined properties were converged.
- Finally, the functional coverage of formal is merged with simulation for comprehensive result. This gives us additional confidence for sign off.
- Compliance feature with single lane was already verified and certified. We adopted FPV for dual lane and no bugs were found.

Formal and Simulation coverage merge



Name	Combined Average Grade	Combined Covered	Combined Status Grade	Overall Average Grade	Overall Covered	Formal Average Grade	Formal Covered
(no filter)	(no filter)	(no filter)	(no filter)	(no filter)	(no filter)	(no filter)	(no filt
USB3.1_Link_Layer	0.53%	40 / 1510 (2.65%)	12.2%	0%	0 / 1510 (0%)	0.74%	40 / 331 (12.08%)
1 7 Link Layer	0.53%	40 / 1510 (2.65%)	12.2%	0%	0 / 1510 (0%)	0.74%	40 / 331 (12.08%)
1.1 7.3 Link Error Rules_slash_Recovery(hst_slash_dev)	0%	0 / 175 (0%)	0%	0%	0 / 175 (0%)	0%	0 / 30 (0%)
1.2 7.4 PowerOn Reset and Inband Reset	0%		0%				
1.3 7.5 Link Training and Status State Machine (LTSSM)	3.7	08%)	18.43%			3	.43%)
1.3.1 LTSSM Coverage_hst_slash_dev	0%		0%			0	
1.3.2 7.5.5 Compliance Mode	33	1%)	90.91%			3	.91%)
1.3.2.1 DSP - default setting for entry to Compliance Mode is disable	0%	0 / 1 (0%)	0%		0 / 1 (0%)	0%	0 / 1 (0%)
1.3.2.2 7.5.5.1 Compliance Mode Requirements	100%	40 / 40 (100%)	100%	0%	0 / 40 (0%)	100%	40 / 40 (100%)
1.3.2.2.1 The port transmits next compliance test pattern continou	100%	2 / 2 (100%)	100%	0%	0 / 2 (0%)	100%	2 / 2 (100%)
1.3.2.2.2 The port transmits the first compliance test pattern cont	100%	2 / 2 (100%)	100%	0%	0 / 2 (0%)	100%	2 / 2 (100%)
1.3.2.2.3 Lane 0 Compliance Test Patterns	100%	18 / 18 (100%)	100%	0%	0 / 18 (0%)	100%	18 / 18 (100%)
1.3.2.2.4 Lane 1 Compliance Test Patterns	100%	17 / 17 (100%)	100%	0%	0 / 17 (0%)	100%	17 / 17 (100%)
1.3.2.2.5 When in Compliance 9 pattern rate change happens fro	100%	1 / 1 (100%)	100%	0%	0 / 1 (0%)	100%	1 / 1 (100%)

- The entry and exit to the Compliance state is verified in the Simulation.
- Formal verification is only applied on the compliance pattern feature.
- Code Coverage can’t be considered since feature is scattered across blocks. Hence, Functional Coverage plays the vital role in Sign-Off.
- To have comprehensive verification sign-off for this feature, coverage metrics obtained from Formal and Simulation are merged and back annotated to Master vPlan.

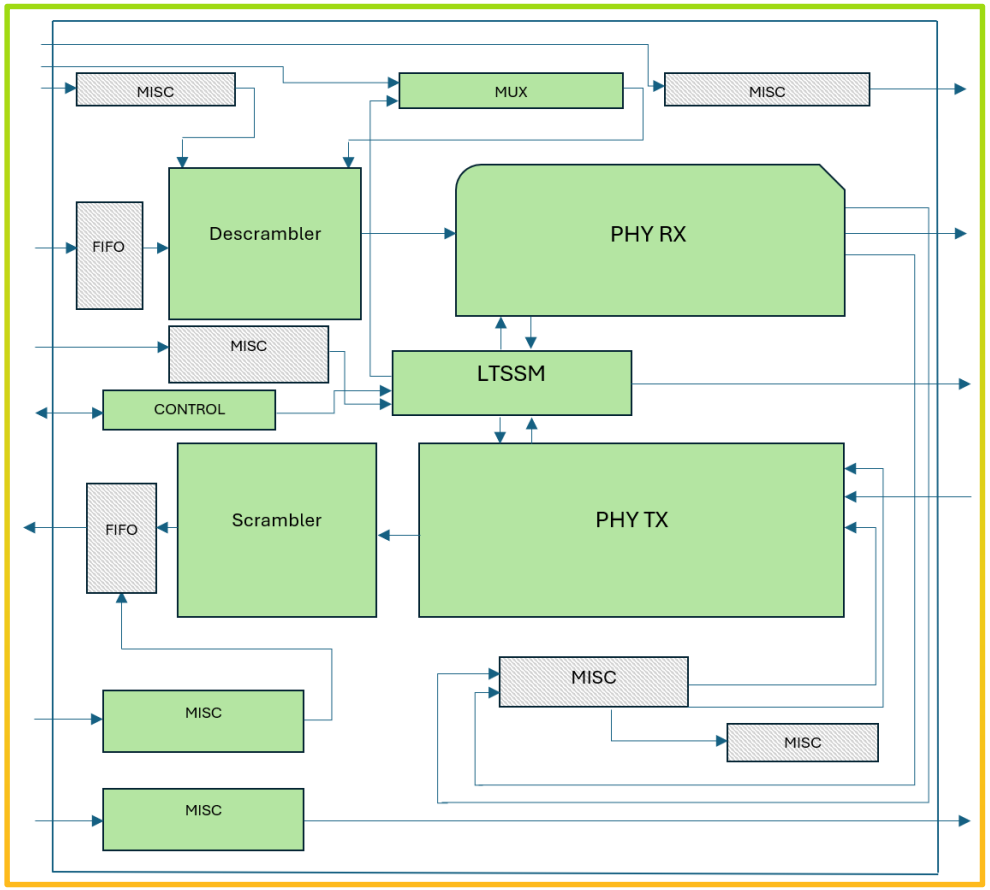
Learnings and Results

- Same methodology is deployed in PCIe L0p Feature Verification.
- The DUT contains about 1400 counters, 1000 Registers and 4 Lakh Gates.

<u>Strategies Deployed Upfront To Reduce complexity of the L0p Feature:</u>

  - Black boxed modules in PHY TOP not contributing to L0p Feature based on Designer's Recommendation.
  - Cut points were applied for the irrelevant signals to the l0p feature.
  - Configurable registers were made constant or tied to zero based on required functionality.
  - IVA and Counter abstractions were applied to reduce the time for convergence.

- These strategies reduced proof run time by 75%



Conclusion

- Feature verification is not impractical using formal, if properly constrained. The rate of covering all the protocol requirements is more feasible through formal.
- Traversing through all the compliance rate changes is a significant achievement proven through this paper which was a tedious task to accomplish in simulation.
- Compliance Feature of USB3.2 controller was successfully signed off with back annotated merged coverage metrics of formal and simulation.
- With this formal approach we were able to left shift the verification by 3 months.

Sakthivel Ramaiah

Design Engineering Architect

Cadence Design Systems

AI

Security

Systems

EDA

Design

62 THE CHIPS TO SYSTEMS CONFERENCE

SPONSORED BY CEDA® IEEE Council on Electronic Design Automation

sigda acm