

Solutions for PCI Express design verification

By Stephen D'Onofrio, Dr. Ambar Sarkar, Jim Tai, and David Lin

Stephen, Ambar, Jim, and David will discuss the problems encountered in PCIe design, present state-of-the-art tools and techniques for verifying compliance and interoperability, and provide an in-depth look at a comprehensive commercial verification IP and compliance suite solution for PCIe.

PCI Express (PCIe) design verification presents significant challenges to System-on-Chip (SoC) developers, both in terms of validating compliance to the PCIe specification and in verifying interoperability with other PCIe design implementations. Ensuring compliance and interoperability requires a robust verification solution that addresses model accuracy, simulation speed, intelligent traffic generation, coverage reports, transaction analysis, compliance test suites, and support for modeling other PCIe design implementations.

A popular specification

In a mere three and a half years since the release of the PCIe¹ specification, PCIe technology has experienced widespread commercial adoption due to its available bandwidth, cost effectiveness, and software compatibility with PCI. With the ability to meet growing bandwidth needs driven by video cards and data storage, PCIe was eagerly anticipated. Indeed, engineers can take advantage of a basic communication lane of 250 MBps in each direction with a x1 implementation and up to 4 GBps with a x16 implementation, an increase of 24x compared to PCI. In addition, significant early investment from companies such as Intel and Dell have accelerated the adoption of PCIe.

Because of compatibility's great importance, PCIe was designed with an architecture that ensures software compatibility so that OSs can boot without modification on a PCIe-based machine. At the same time, there is no expectation on hardware compatibility; most of the derived benefit comes from a redesign of the chip architecture.

PCIe design verification challenges

Unfortunately for chip design and verification teams, the PCIe specification, though well written, is described in documents exceeding a thousand pages in length, containing the unavoidable ambiguities subject to human interpretation.

This standard allows for a wide range of device types, features, and functionality. With PCIe version 2.0 (Gen II) evolving rapidly,

adding yet another layer of complexity, fewer chip designs are implementing 100 percent of the features as defined in the specification. To help ensure compliance, PCI-SIG, the industry controlling organization for the PCI Express specification, created a compliance checklist² to help maximize the likelihood of design interoperability and conform to current industry standards.

Traditionally, compliance and interoperability with other compliant devices comprise the two key elements to verify a PCIe implementation from a hardware perspective. Compliance verification ensures that the design adheres to the features and functionality as defined in the specification from standards bodies. Interoperability verification ensures that designs can interoperate or communicate with other devices in the system using the interface standard.

Compliance and interoperability testing

In the past, the most common method for testing interoperability was the *plugfest*, in which design teams from different companies brought their products together and tested, one-on-one, how well they worked with each other. Unfortunately, plugfests are postsilicon, meaning the design has already been committed before it's possible to establish confidence in it. It is preferable to perform as much testing for both compliance and interoperability during the *presilicon* verification stage.

However, too many companies have learned the hard lesson that compliance does not necessarily guarantee interoperability. A typical PCIe verification plan must incorporate a more stringent verification strategy than just compliance. As an example, consider the requirement of testing back-to-back traffic for each possible combination of TLP packet types. This requirement is not a part of the PCIe Compliance Checklist, but should be included in a verification plan involving PCIe interfaces.

Commercial Verification IP

One way to reduce risk of incompatibility and poor functionality is to use silicon-proven third-party Verification IP (VIP) components. Using proven VIP helps projects start more quickly and increases confidence in the verification environment. Conversely, using poor quality VIP will slow down the overall verification effort and may even result in producing false positive testing.

Before investing in VIP, a design team should know how many successful designs used the VIP. The potential VIP provider

should give examples of how to set up some complex scenarios.

Offerings from various vendors may differ, but state-of-the-art verification IP solutions such as those offered by Denali Software³ (Figure 1) will typically provide:

- **Bus Functional Model (BFM)** to encapsulate the complete features and functionality of the specification even as it continues to evolve (for example, from 1.0a → 1.1 → 2.0)⁴, with the ability to initiate and respond to interface traffic. The BFM element must also include the ability to inject erroneous transactions to ensure proper error recovery from the design.
- **Assertion Library** to dynamically monitor device behavior against the protocol rules defined in the specification. For example, VIP for PCIe must contain much more than 1,200 unique assertions to validate that a given design complies with the PCIe specification.
- **Compliance suite** to exercise specific functionality and corner cases in the specification, including compliance checklist items provided by the standards organizations. Comprehensive suites should contain several thousand tests to exercise the design. For example, Denali's PureSuite Compliance Test suite for PCIe contains more than 8,000 unique tests to exercise and verify all aspects of a given PCIe design.
- **Test sequences and coverage metrics** to generate specific traffic patterns for functional verification. Together with a strong coverage model, this enables rapid generation of application-specific traffic for system-level verification above and beyond compliance and interoperability testing.
- **Debug solutions** to support transaction-level debug and analysis of data and transactions at various layers of the protocol.
- **EDA integration and portability** to support easy deployment into all commercial verification tools and languages. This requirement is critical since the verification IP often becomes the central and shared element of interoperability verification involving third party designs. For example, the highly portable nature and widespread deployment of PureSpec has led to its use across the industry as a leading model to ensure PCIe quality and interoperability.

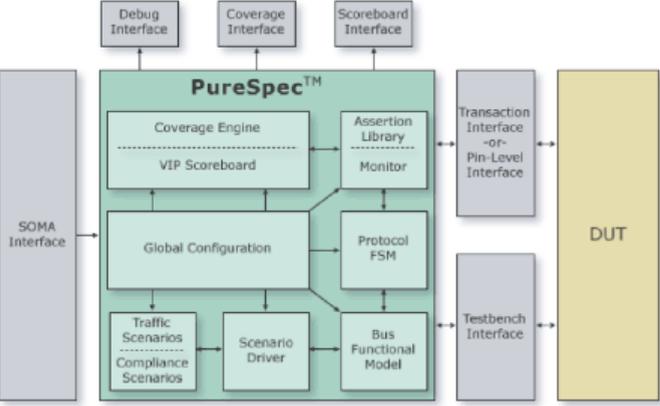


Figure 1

VIP in use: Examples from real life

Increasingly, projects are incorporating PCIe design IP in their SoC implementations. Unfortunately, the quality of these design IPs often gives cause for concern. To make matters worse, the design and verification teams may not have a sufficient time to grasp all the complexities of the protocol.

By using a compliance suite to qualify the design IP, a verification team can mitigate the corresponding risks. The numerous compliance and interoperability tests can be used to check the design IP,

and an accurate compliance coverage report can be generated. A default testbench in the target design language, such as Verilog, must also be included to avoid wasting time on creating an infrastructure from scratch when verification is the real goal. By instantiating the actual Design Under Test (DUT) IP into a provided test compliance solution, clients can quickly evaluate design IP from various sources.

In addition to the compliance testing, a team can also get a jump start in interoperability verification by using PCIe verification IP even when only partial implementations are available. By substituting a BFM in place of a yet to be developed register transfer level block, one can run system-level simulations (Figure 2).

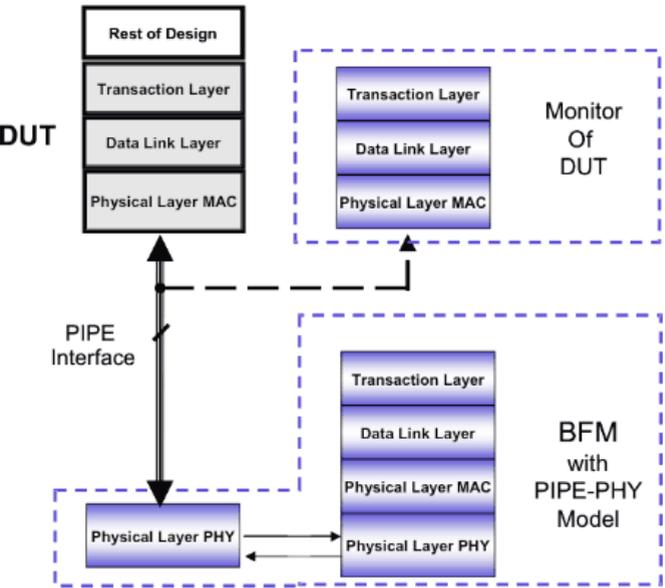


Figure 2

In the case of one design team, the SERDES implementation did not become available until much later during the project. To work around this, the analogous VIP components were hooked up in PHY Interface for PCIe (PIPE)⁵ mode directly to the rest of the DUT. Even with a partial PCIe implementation, the team verified the bring-up sequence by running typical scenarios in a relatively short amount of time. Once the Physical Layer (PHY) implementation became available, it was added into the testbench. Simultaneously, the VIP PIPE mode components were replaced with their counterparts in serial mode (Figure 3).

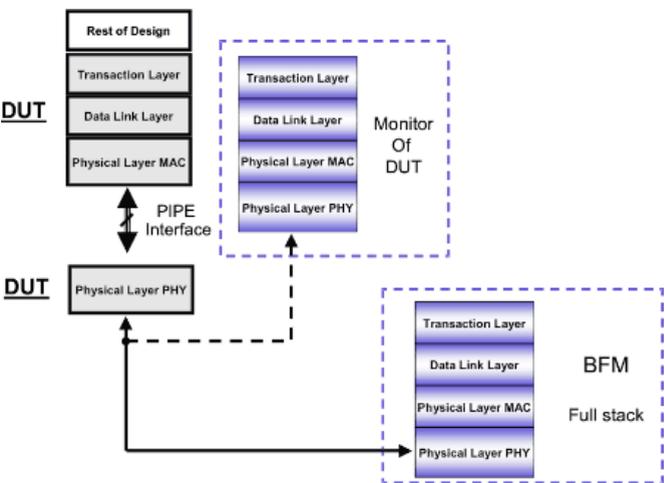


Figure 3

The internal state of a PCIe device is complex and represented by the VIP transactors as internal register and memory shadow objects. Callback mechanisms are provided for invoking user-defined methods when these state objects are accessed. These shadow objects proved critical for the behavioral prediction as well as the generation of intelligent responses by the verification environment.

For example, when the PureSpec Root Complex (RC) receives a memory read request, the completion TLP to the Endpoint (EP) requestor can be created automatically by virtue of the shadow object availability. Since it had the shadow register contents of the EP ports, the testbench environment could predict automatically where the return packet should go, and whether it needed to do split completion, and so on. These features of the PCIe VIP enable clients to create conditions for a variety of complex corner cases.

Conclusions

PCIe is a complex protocol, and with the evolving PCIe version 2.0 (GenII) around the corner, presilicon verification is critical. Using state-of-the-art VIP solutions, such as Denali's PureSuite and PureSpec for PCIe, can help accelerate the design verification process.

Stephen D'Onofrio is a principal consulting engineer at Paradigm Works. His primary responsibilities include leading verification teams, writing verification plans, building verification environments, and implementing tests at various client sites. Prior to his current position, he worked as an ASIC project lead at ERSI and a diagnostic engineer at Datacube. He holds a BS in Electrical Engineering from the University of Massachusetts.



Dr. Ambar Sarkar is currently a chief verification technologist at Paradigm Works. His primary focus is functional verification, and he enjoys taking the latest innovations in the industry and applying them toward the success of client projects. He has a PhD in Computer Science from the University of Virginia.



Jim Tai is a principal consulting engineer at Paradigm Works. He has been in the chip verification consulting industry since 1996. Jim is involved in all aspects of verification: selecting proper methodology, writing verification plans, building verification environments, and writing scripts and tests. He holds an MS in Electrical and Computer Communication Networks from Worcester Polytechnic Institute.



David Lin joined Denali in July 1997 and is currently vice president of applications engineering. His team's mission is to ensure customer satisfaction through the successful adoption of Denali's technology into customers' environments. He is also responsible for developing and enhancing key memory vendor partnerships. Preceding Denali, David held senior engineering positions at Synopsys and Mitsubishi Electric, and also served on the IEEE 1076.4 VITAL standards definition committee. He holds a BS in Computer Engineering from Princeton University.



To learn more, contact the authors at:

Paradigm Works, Inc.

300 Brickstone Square • Suite 104 • Andover, MA 01810

Tel: 978-824-1400 • Fax: 978-824-1401

E-mail: info@paradigm-works.com

Ambar.Sarkar@paradigm-works.com

Jim.Tai@paradigm-works.com

Stephen.Donofrio@paradigm-works.com

Website: www.paradigm-works.com

Denali Software Inc.

1850 Embarcadero Road • Suite B • Palo Alto, CA 94303

Tel: 650-461-7200 • Fax: 650-461-7209

E-mail: info@denali.com

david@denali.com

Website: www.denali.com

References

- [1] PCI Express Base Specification Revision 1.1, PCI-SIG
- [2] PCI Express 1.0a Root Complex Checklist, PCI-SIG
- [3] PureSpec-PCIe User's Guide, Denali Software
- [4] PCI-SIG Developer's Conference, PCIe 2.0 Architectural Extensions, PCI-SIG
- [5] PHY Interface for PCI Express (PIPE) Architecture Gen 2 (Draft), Intel Corporation