SIP Verification Challenges

Mike Bartley, CEO, Alpinum Consulting | Andrew Bond, Axelera AI

Abstract

- System In Package (SiP) is a system built from multiple Chiplets. Verifying a SiP design introduces multiple challenges which have been described precisely in this presentation. We have proposed solutions and recommendations to all such challenges. Proposed solutions and recommendations are analysed and quantized against all verification metrices, techniques and flows to draw a conclusion on methodologies for SiP verification.

Outline

- Introduction and Overview - Chiplet based Systems Verification
- Scope of Discussion – SiP Verification White Paper
- Overview of SiP Verification Challenges
- Main SiP Verification Challenges Discussions & Recommendations
- Next Steps & Future Work
- Conclusion
- Questions

Introduction and Overview – Chiplet based Systems Verification

- A Chiplet is a functional integrated circuit.
- A System in Package (SiP) is built from multiple Chiplets.
- SiPs can be of different types based on the Chiplet dies integrated into the package:
  - Heterogeneous SiP:
    - Composed of different types of Chiplet dies (e.g., compute, network, memory, etc.)
    - May include dies designed on different process nodes
    - May involve dies from different manufacturers
  - Homogeneous SiP:
    - Composed of similar Chiplet dies (e.g., compute + compute)
    - Typically designed on the same process node
    - Likely from the same manufacturer
- Conventional verification techniques (simulation, emulation, formal) used for SoCs are also applied to SiPs.
- Additional verification challenges must be considered for Chiplet-based systems.
- Similar to SoC verification, it is assumed that:
  - Underlying IPs, protocols, and subsystems are pre-verified at their respective levels.
  - For SiPs, each Chiplet's protocol-level verification is assumed to be completed at the Chiplet level.

Scope of Discussion – SiP Verification White Paper

- In this presentation we are discussing SiP Verification challenges, identified and discussed in the white paper “System In Package Verification”
- This White Paper discusses the Status of SiP Verification
- Discusses SiP Verification Challenges and propose recommendations to address these challenges

Overview of SiP Verification Challenges

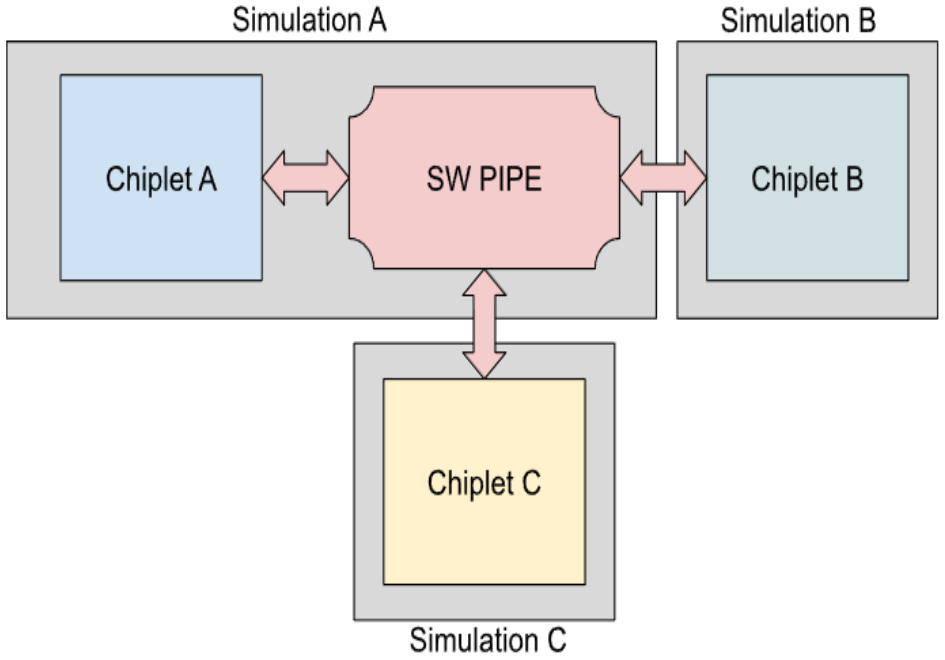
- **Challenges:**
- System Simulation of SiP - Due to Chiplets originating from different vendors
- Protocol challenges – Heterogenous and Homogeneous Chiplets
- Scalability
- Clock, power and reset signals verification across different layers
- Coherency issues across Chiplets
- Security
- IP and VIP deliverables enablement
- Defining verification Sign off criteria for SiP
- Create a criteria to define a good verified Chiplet for SiP Integration & Verification

SiP Verification Challenges (System Simulation multiple Vendors)

- **Challenges & Discussions**
  - Conventional SOC Integration Verification considers IPs as Soft or Hard
  - Intent in terms of SiP is somewhat similar to SOC
  - Importance of Design and Coding Styles used
  - Simulation and Tooling conventions
  - Licensing and Technical changes
  - IPs from multiple vendors work together when integrated
  - Reliance on Interface Protocols
- **Recommendations**
  - Providers should supply details to compile in a standalone resource library
  - Designs should be x-propagate tolerant
  - Zero delay RTL simulations
  - Standard adoption for encrypted designs
  - Minimal set of design lint rules should be defined and followed by all providers

SiP Verification Challenges (System Simulation Scalability)

- **Challenges & Discussions**
  - Designs are getting bigger and bigger, simulating large designs are already a big challenge in conventional SOCs
  - More memory and compute requirements are required to simulate the deigns
  - Emulation instead of Simulation
  - Simulators are fundamentally single threaded programs
  - Purpose of verification and abstraction layers
  - Testing in perspective of System, Subsystem/Core, IP and block levels distinguishes the scope
  - Multi-Simulation system in multithreading processing, Split Design
  - Simulation of each Chiplet can run independently and with max performance
  - This PIPE2API mechanism can facilitate with development of compliance



- **Recommendations**
  - Development of an independent, interoperable standard will allow SIP designers to split designs over multiple processors for Simulations

SiP Verification Challenges (SiP & Pre-Silicon Verification Env)

ALPINUM CONSULTING

- **Challenges & Discussions**
  - Verification Infrastructure, Tools, methodologies, languages and include definition of Sign off criteria
  - Reuse of Verification environment
  - Abstraction Layers verification
  - Conventional SOCs verification
  - Aspects and Considerations required to help to integrate and reuse Chiplet level verification to system level
  - A Shift in legacy thought process to fit broader Chiplets verification environment to adopt standards
- **Recommendations**
  - Use 100% UVM compliant verification environments
  - Define Clear partition and modularized approach while building mixed UVM & Non-UVM compliant Environments
  - Partition compile for efficient execution and debug
  - Sequences and Tests, Small and focused. Use layered approach

SiP Verification Challenges (Coverage Closure Criteria)

ALPINUM CONSULTING

- **Challenges & Discussions**
  - Hard and challenging to close coverage with so many Chiplets in a SiP
  - Importance of coverage selection criteria for SiP to sign off verification i.e. Each Chiplet closed coverage at their level
  - Coverage on new blocks not covered under individual Chiplets , glue logic, integration configuration and specific SiP features to be closed at SiP level.

- **Recommendations**
  - Focus to close coverage on new blocks and glue logic
  - Close coverage on all possible SiP configurations for functional and code level coverage
  - Integration coverage – covering all data paths i.e. all Chiplets are active and driving traffic
  - Comprehensive verification approach, focusing on defining and verifying system level scenarios, performance verification and security verification. A comprehensive framework covering all integration logic, configurations and data paths involved, for coverage collection

SiP Verification Challenges (System Integration)

- **Challenges & Discussions**
  - Coherency across Chiplets – maintaining cache coherency across multiple Chiplets in Heterogeneous systems
  - Interrupt function and performance (latency) across SiP
  - Data bandwidth & Latency – Data transfer b/w Chiplets
  - Error rates and Stability of Connections – BER and signal integrity issues
  - Ever – Changing Scenarios (Dynamic Workloads) – Adaptability in resource allocation and power management

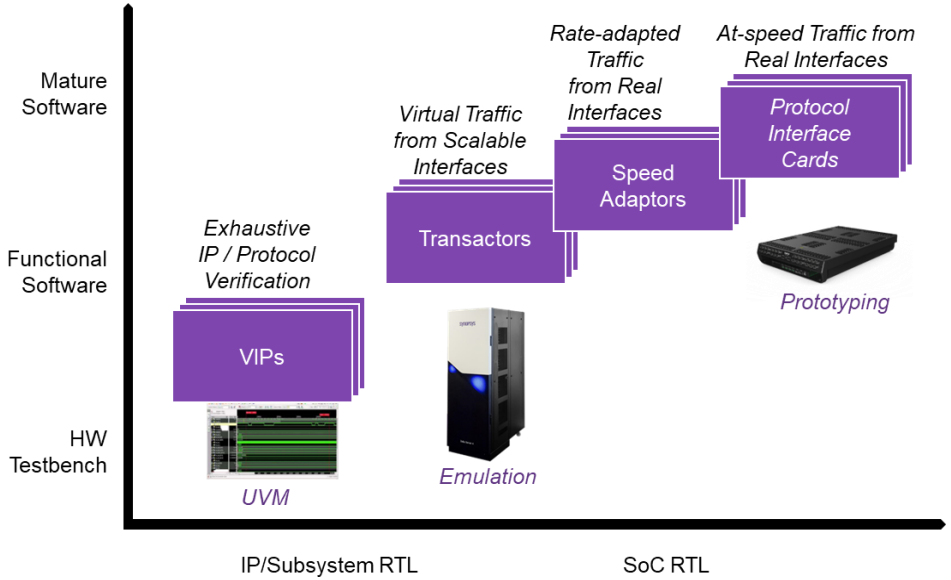
- **Recommendations**
  - Use standard interconnect CXL, CCIX Protocols
  - Optimize interrupt controllers, use low latency interconnects such as Advanced Interface bus (AIB) and Bunch of Wires (BoW) to enhance communication speed & efficiency
  - Use high speed interconnect technologies i.e. HBM and SerDes for data transfer
  - Use Error correcting codes (ECC) and signal integrity techniques i.e. equalization, pre-emphasis
  - Adopt dynamic resource management and adaptive power management

SiP Verification Challenges (Security)

- **Challenges & Discussions**
  - Security of SiP – Security and Trust challenges
  - Hardware Integrity
  - IP Theft
  - Integration and supply chain risks
  - Additional Security Threats
  - Emerging Threat Vectors
- **Recommendations**
  - Mitigate Hardware Integrity threats – Multifaceted approach
  - IP Theft mitigation – Using Encryption Techniques
  - Mitigate Integration and supply chain risks - Trusted partnership and vendors
  - Mitigate Additional security risks – Masking techniques to obscure sensitive data
  - Mitigate Emerging Threat Vectors – Use of AI to monitor and detect anomalies

SiP Verification Challenges (IP & VIP deliverables)

- **Challenges & Discussions**
  - Chiplets based system – Importance of IPs and VIPs
  - Individual IP verification integration into Chiplet level verification
  - IP level to subsystem level, Emulation or SOC prototyping solution
- **Recommendations**



  - Follow Standard UCIe verification components
  - Use consistent SI-PI models – for Signal and Power integrity check
  - Take advantage of PVE (platform verification Env) or similar standard - UVM Test Bench
  - Model and simulate end to end, Emulation models , Synopsys Zebu, Prototyping platform HAPS

SiP Verification Challenges (Functional Verification Compliance)

- **Challenges and Discussions**
  - What is needed for functional verification compliance
  - What “good looks like” for a verified Chiplet
  - SiP is essentially a heterogenous env.
  - Define clear metrices for verification completion
  - Limitations due to SiP multi – die designs
  - Limitations due to different vendors using different methodologies
- **Recommendations**
  - Establish Compliance Test Suite (CTS)
  - Establish set of measurable verification goals
  - Check before integrating, Predefined verification checklist i.e. functional correctness of interfaces Power intent and performance benchmarks and collaterals i.e. Verification and Coverage reports, debug database

Next Steps & Future Work

- White paper is submitted to OCP for review
- Ongoing work to add more details
- Collaborate with industry leading EDA, IP, VIP suppliers to fine tune on the challenges and recommendations

Conclusion

- Multiple SiP Verification Challenges and solutions are discussed
- Recommendations have been drawn based on practical aspects of SiP verification for such challenges
- Techniques and recommendations for various challenges are based on verification approaches used in conventional SOC’s verification with added considerations for the SiP based designs
- Recommendations presented are sets of guided steps to be applied and the conventions and techniques as guidelines to the Chiplet community