Pragmatic Formal Verification Methodology for Clock Domain Crossing

Aman Kumar, Infineon Technologies
Muhammad U.H. Khan & Bijitendra Mittra, Cadence Design Systems
## Agenda

<table>
<thead>
<tr>
<th></th>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Verification challenges</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Technical background</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>Methodology development &amp; implementation</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>Results and summary</td>
<td>18</td>
</tr>
</tbody>
</table>
Agenda

1. Verification challenges
2. Technical background
3. Methodology development & implementation
4. Results and summary
Clock domains are increasing with increasing complexity

Number of Asynchronous Clock Domain on ASIC Projects

Source: Wilson Research Group Functional Verification Study 2022

3 – 4
Average number of clock domains on ASIC designs
CDC issues are a major reason for expensive respins

- CDC issues are 3rd major reason for Silicon respins

Source: Wilson Research Group Functional Verification Study 2022
Agenda

1. Verification challenges 3
2. Technical background 6
3. Methodology development & implementation 10
4. Results and summary 18
A clock domain (CD) is a region of synchronous logic with exactly one clock. Most real-life designs operate on multiple clocks (for power and performance reasons). A clock domain boundary arises when the clocks change. Signals crossing clock domains must be synchronized to avoid metastability effects! Metastability modeling → creating setup/hold violations.

Source: Cadence JasperGold CDC user guide
CDC issues

Structural violations

- Missing synchronizers
- Combinational logic on CDC path
- Structural glitch

CDC protocol violations

- Standard synchronization scheme-specific transfer protocol related issues
- Custom synchronization scheme-specific issues

Data coherency issues

- Convergent/divergent/re-convergent design structures

Reset domain crossing

- Reset related violations
Conventional CDC verification

- **Design Specification**
  - **RTL Design**
    - CDC Constraints
    - RTL Code
    - **Structural Analysis**
      - **Functional CDC Analysis**
        - Sign-off by Designer
  - **Functional Verification**
    - **Simulation with MSI**
      - **Code & Functional Coverage Closure**
        - Sign-off by Verifier

- **Verification Plan**
  - **Test cases**
  - **Testbench Creation**
    - **Functional Verification**
      - **Code & Functional Coverage Closure**
        - Sign-off by Verifier

- **MSI** – Metastability Injection
- **CDC** – Clock Domain Crossing

- **Missing Constraint Validation**
- **Absence of Functional Analysis with MSI**
- **No checks for user-defined synchronizers**
- **Missing Formal Functional Verification with MSI**
- **Inaccurate Metastability Modeling**
- **No Coverage Model for CDC Closure**
Agenda

1. Verification challenges 3
2. Technical background 6
3. Methodology development & implementation 10
4. Results and summary 18
Proposed CDC verification flow

What are the benefits?

CDC Structural Analysis

CDC Functional Analysis with Constraint Validation

Metastability Analysis

CDC Clean RTL

Sign-off by Designer

Complete CDC Sign-off

CDC Clean RTL

Formal Functional Verification

Formal Functional Verification with MSI

Sign-off by Verifier

Simulation with MSI

Formal Functional Coverage Closure

CDC Coverage Closure

System Verilog Assertions

Formal Verification Environment Setup

CDC Constraints

RTL Design

RTL Code

Design Engineer

Verification Engineer

Design Specification

Verification Plan
Proposed CDC verification flow

1. Design Specification
   - Design Engineer
   - RTL Design
     - CDC Constraints
     - RTL Code
       - CDC Structural Analysis
         - Automated checks
         - CDC Functional Analysis with Constraint Validation
           - Metastability Analysis
             - CDC Clean RTL
               - Sign-off by Designer
               - Complete CDC Sign-off
   - Verification Plan
     - Verification Engineer
     - System Verilog Assertions
       - Formal Verification Environment Setup
         - Formal Functional Verification with MSI
           - Simulation with MSI
             - Formal Functional Coverage Closure
               - Sign-off by Verifier
               - CDC Coverage Closure
                 - CDC Clean RTL
                   - Sign-off by Designer
                   - Complete CDC Sign-off

2. Design Engineer roles:
   - RTL Design
   - CDC Constraints
   - RTL Code

3. Verification Engineer roles:
   - Verification Plan
   - System Verilog Assertions
   - Formal Verification Environment Setup
   - Formal Functional Verification with MSI
     - Simulation with MSI
       - Formal Functional Coverage Closure
         - Sign-off by Verifier
         - CDC Coverage Closure
           - CDC Clean RTL
             - Sign-off by Designer
             - Complete CDC Sign-off
Proposed CDC verification flow

- Design Engineer
  - Design Specification
    - RTL Design
      - CDC Constraints
      - CDC Clean RTL
    - RTL Code
      - CDC Functional Analysis
        - Automated checks
        - Checks for user-defined synchronizers
      - CDC Functional Analysis with Constraint Validation
        - Metastability Analysis
      - CDC Clean RTL
    - CDC Structural Analysis
      - Complete CDC Sign-off
        - Sign-off by Designer
        - Sign-off by Verifier
    - Formal Functional Verification
      - Formal Functional Verification with MSI
      - Simulation with MSI
      - Formal Functional Coverage Closure
    - System Verilog Assertions
      - Environment Setup
      - Assertions
    - Verification Plan
      - Verification Engineer
      - CDC Clean RTL
      - Formal Functional Verification
      - Formal Functional Coverage Closure
Proposed CDC verification flow

Design Engineer

- Design Specification
  - RTL Design
    - CDC Constraints
      - Automated checks
      - Checks for user-defined synchronizers
    - RTL Code
      - CDC Structural Analysis
        - CDC Functional Analysis with Constraint Validation
      - Metastability Analysis
    - CDC Clean RTL
      - CDC Clean RTL

Verification Engineer

- Verification Plan
  - Formal Verification Environment Setup
    - Formal Functional Verification
      - Formal Functional Coverage Closure
        - Sign-off by Verifier
          - CDC Coverage Closure
            - Simulation with MSI
              - Formal Functional Verification with MSI
                - Sign-off by Designer
                  - CDC Coverage Closure
                    - Sign-off by Designer
Proposed CDC verification flow

Design Engineer

RTL Design

CDC Constraints

RTL Code

Design Specification

Verification Engineer

Verification Plan

Formal Verification Environment Setup

System Verilog Assertions

Formal Functional Verification

CDC Clean RTL

Complete CDC Sign-off

Sign-off by Designer

Sign-off by Verifier

CDC Coverage Closure

Formal Functional Verification with MSI

Simulation with MSI

Formal Functional Coverage Closure
**Metamodelling**

- **Spec layer**
  - **Model of Things (MoT)**
    - **Formalized specification**
  - **Template of Property (ToP)**
    - **Python**

**Property layer**
- **Generation Framework**
- **Target Code**
  - **SVA/SV**

**Configurations**
- **CLK1**
- **CLK2**
- **CDC pair information**

**Synchronizer type details**

**BLACKBOX**

**SVA/SV**

```verilog
property data_stable;
@ (posedge clk1) disable iff (!rst_n)
$stable (data_i) [*2];
endproperty
```

**Coverage**

```verilog
covergroup cg @ (posedge clk)
  cp_src: coverpoint sig_src
  cp_dest: coverpoint sig_dest
  cp_cdc pair: cross cp_src, cp_dest
```
<table>
<thead>
<tr>
<th>Type</th>
<th>Analysis Used</th>
<th>Bug Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTL bug</td>
<td>Structural analysis</td>
<td>Missing synchronizer for CDC signal</td>
</tr>
<tr>
<td>RTL bug</td>
<td>Structural analysis</td>
<td>Missing synchronizer for RDC signal</td>
</tr>
<tr>
<td>RTL bug</td>
<td>Structural analysis</td>
<td>Combinational logic on the CDC path</td>
</tr>
<tr>
<td>RTL bug</td>
<td>Structural analysis</td>
<td>Combinational logic on the RDC path</td>
</tr>
<tr>
<td>RTL bug</td>
<td>Structural analysis</td>
<td>Reset signal converged before reaching the destination unit</td>
</tr>
<tr>
<td>RTL bug</td>
<td>Functional analysis</td>
<td>Wrong signal configuration (signal not static)</td>
</tr>
<tr>
<td>RTL bug</td>
<td>Functional analysis</td>
<td>Signal not stable enough to be captured correctly by destination unit</td>
</tr>
<tr>
<td>Testbench bug</td>
<td>Functional analysis</td>
<td>Input pulse was more than 1 cycle wide (pulse synchronizer)</td>
</tr>
<tr>
<td>Testbench bug</td>
<td>Functional analysis</td>
<td>Data loss because of incorrect clock frequencies</td>
</tr>
<tr>
<td>Testbench bug</td>
<td>Metastability analysis</td>
<td>Assertion didn’t handle the extra delay due to metastability propagation</td>
</tr>
<tr>
<td>Tool bug</td>
<td>MSI model generation</td>
<td>MSI model was not getting generated for simulation</td>
</tr>
</tbody>
</table>
CDC verification on chip level

- MSI model integration to the simulation testbench
- Simulation waveform
- CDC coverage analysis
Summary

Early detection of CDC bugs
- Detection of bugs at the pre-silicon verification phase
- Less effort/time to fix the bug
- Saves money by avoiding costly re-spin

Features
- Uses both formal & simulation techniques
- High-quality design ensured with coverage analysis
- Automated assertion checks

Design & verification linkage
- Bridges the gap between structural and functional analysis
- Defines a CDC sign-off flow for both design and verification

Future work
- Detection of more synchronizer schemes
- Automated testbench generation for MSI in simulation
- Application in power-aware

Pragmatic CDC formal verification