# Don’t Forget the Protocol! A CDC Protocol Methodology to Avoid Bugs in Silicon

Abdelouahab Ayari, Mentor, a Siemens Business
Sukriti Bisht , Mentor, a Siemens Business
Sulabh Kumar Khare, Mentor, A Siemens Business
Kurt Takara, Mentor, a Siemens Business

Mentor®
A Siemens Business

accellera SYSTEMS INITIATIVE

2019 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION EUROPE

# Introduction

- **CDC issues**: 2nd most common reason for silicon re-spins
  - **Structural CDC Verification**
    - Use of synchronizer to essentially reduce the probability of metastability
    - Good understanding in industry (part of some  industry standards like DO-252)
    - Widely used in industry
  - **Functional CDC Verification**
    - Synchronizers has to meet functional requirements (CDC Protocols)
    - No large awareness in industry

# If CDC Protocol Verification is Skipped

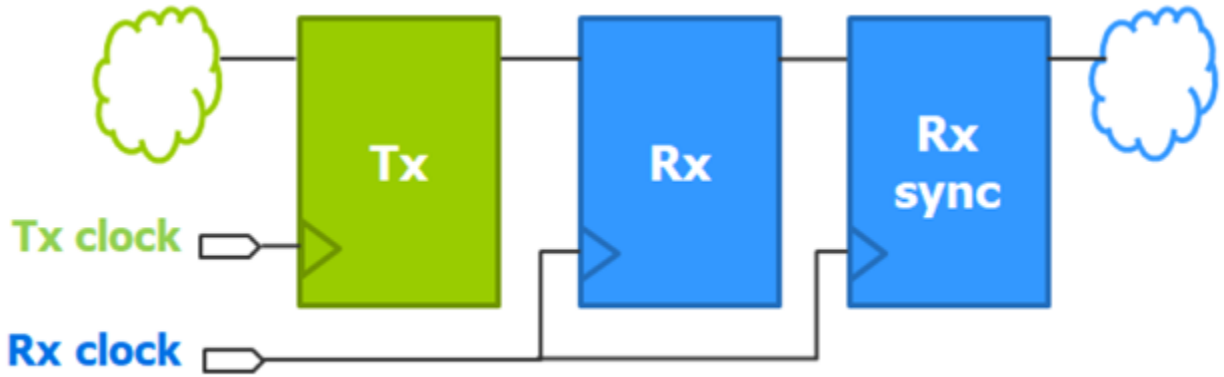
- **Structural CDC checking  alone is not enough**

- **Risks**
  - Lose of data
  - Propagation of metastability (→ corruption of data)

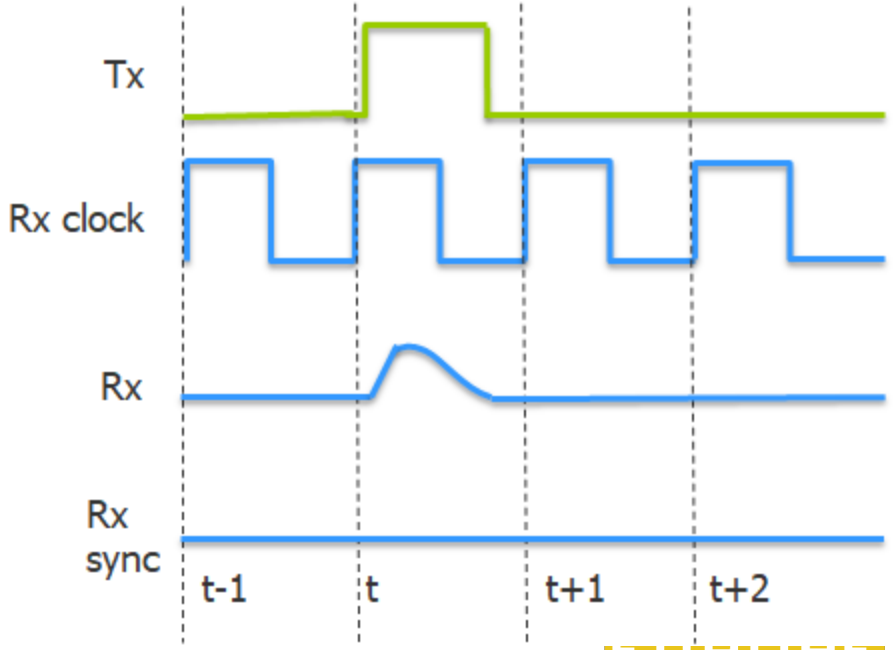
# Risks: Loss of Data

- **Case of a 2DFF Synchronizer Protocol Violation**
  - TX Data stable for less than two (NUM_CYCLES) clock cycles
- **What happen**
  - Data is lost

```
property data_stable_prop(data, clock, reset, areset, NUM_CYCLES);
    @(posedge clock) disable iff(areset)
  ##1 !reset && $changed(data) |=> $stable(data)[*(NUM_CYCLES-1)];
endproperty
```

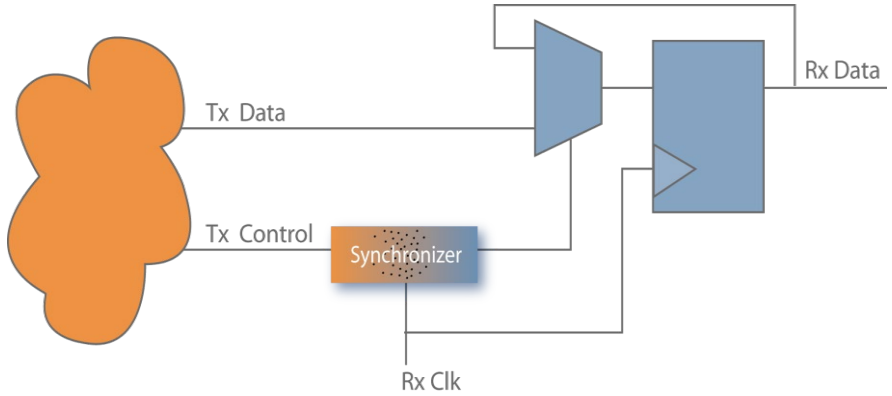



Two DFF synchronizer



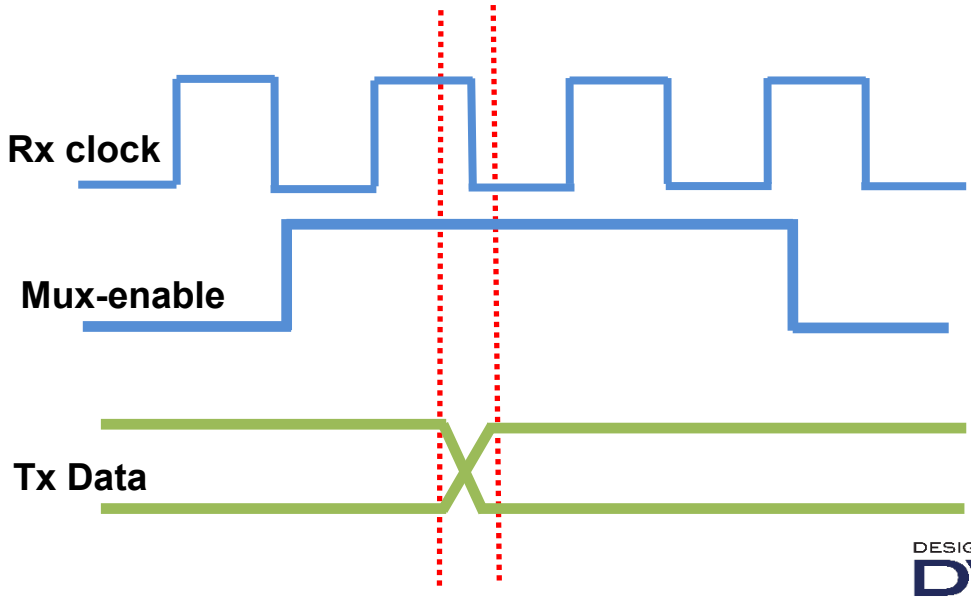
# Risks: Propagation of Metastability

- **Case of a Protocol Violation**
  - Mux-enable is asserted and
  - TxData is changing in the critical time window of the receive clock RxClk



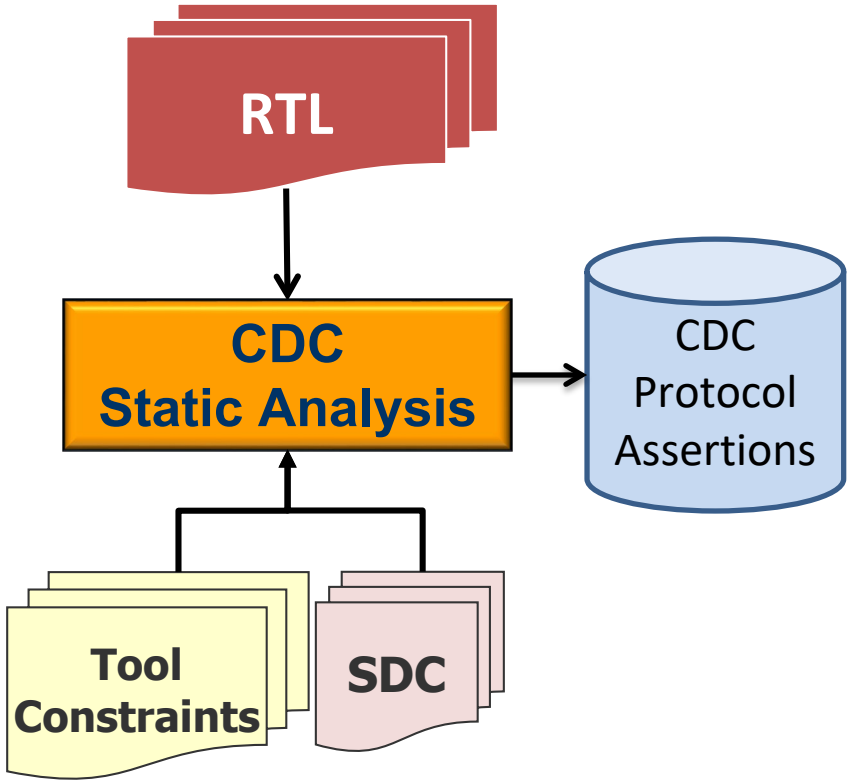
Data-Mux (DMUX) Synchronizer

- **What happen**
  - ***Metastability could be propagated***
  - *Corruption of RxData*

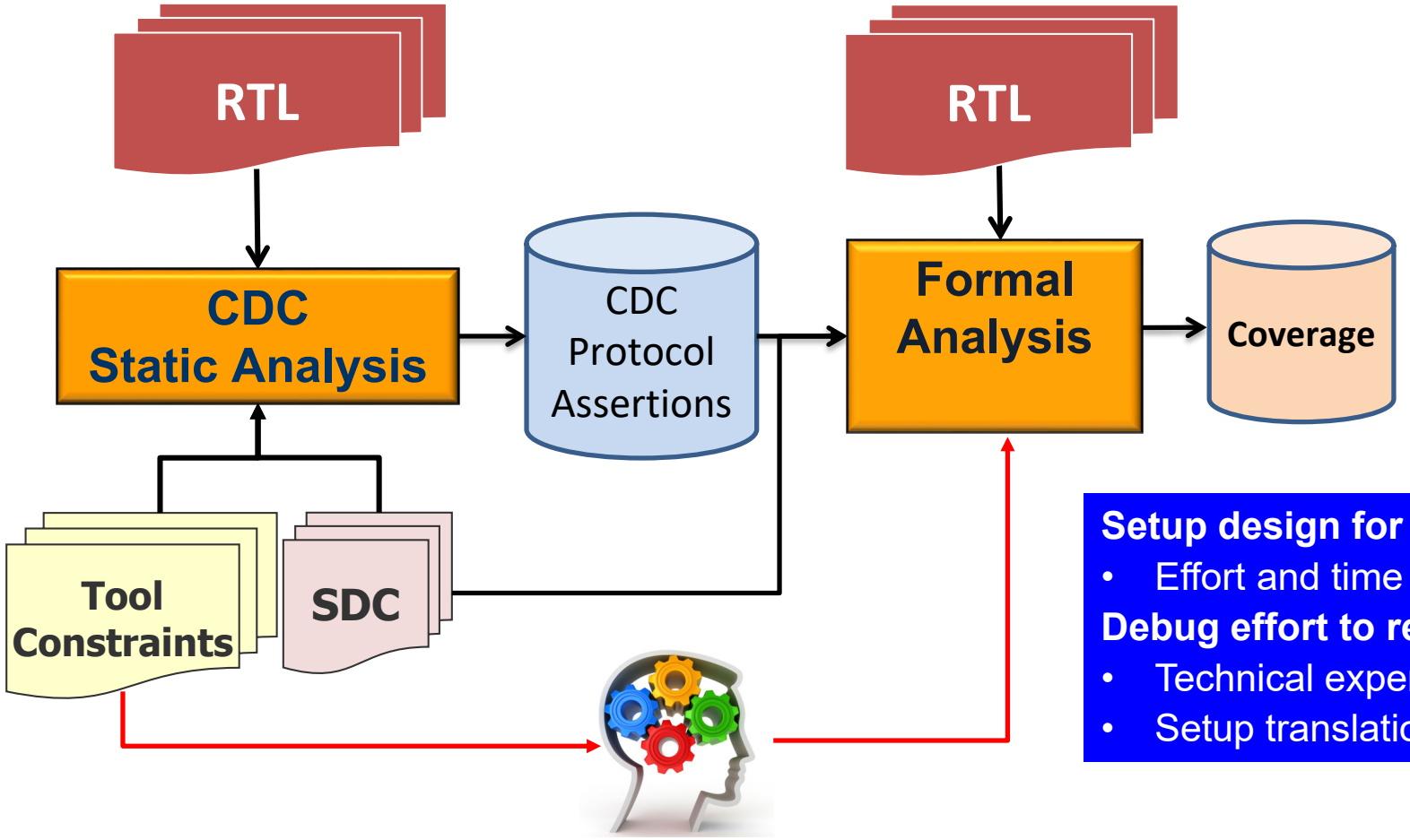


# CDC Protocol Verification is a MUST !!

# Challenge of Existing Verification Methodology



# Challenge of Existing Verification Methodology



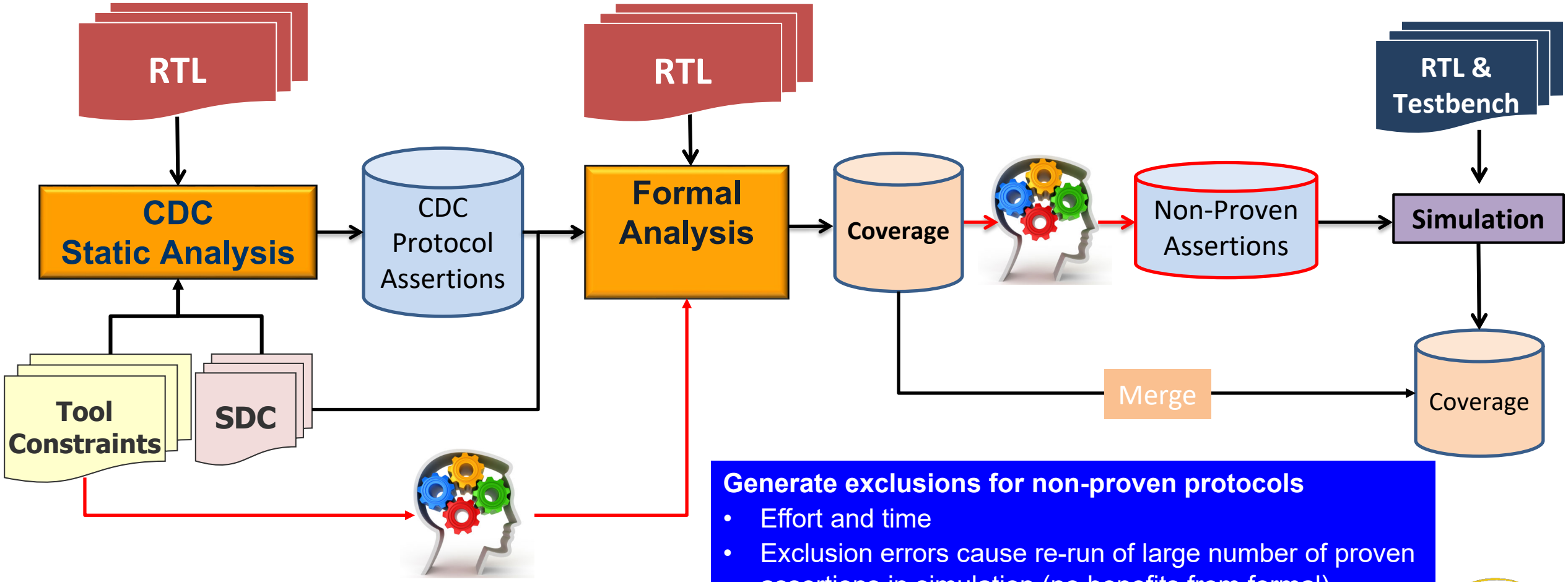

**Setup design for Formal**

- Effort and time

**Debug effort to review firings**

- Technical expertise of both environments
- Setup translation errors cause false violations

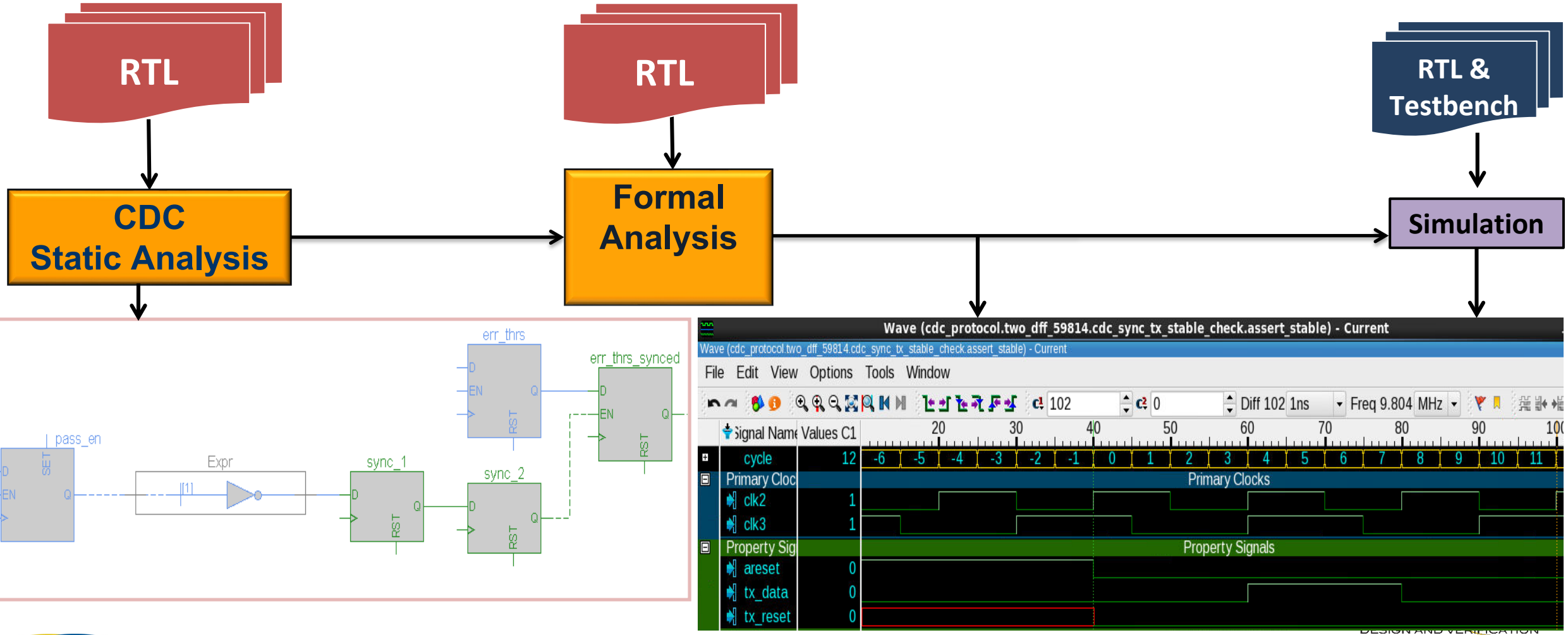
# Challenge of Existing Verification Methodology




**Generate exclusions for non-proven protocols**

- Effort and time
- Exclusion errors cause re-run of large number of proven assertions in simulation (no benefits from formal)

# Challenge of Existing Verification Methodology



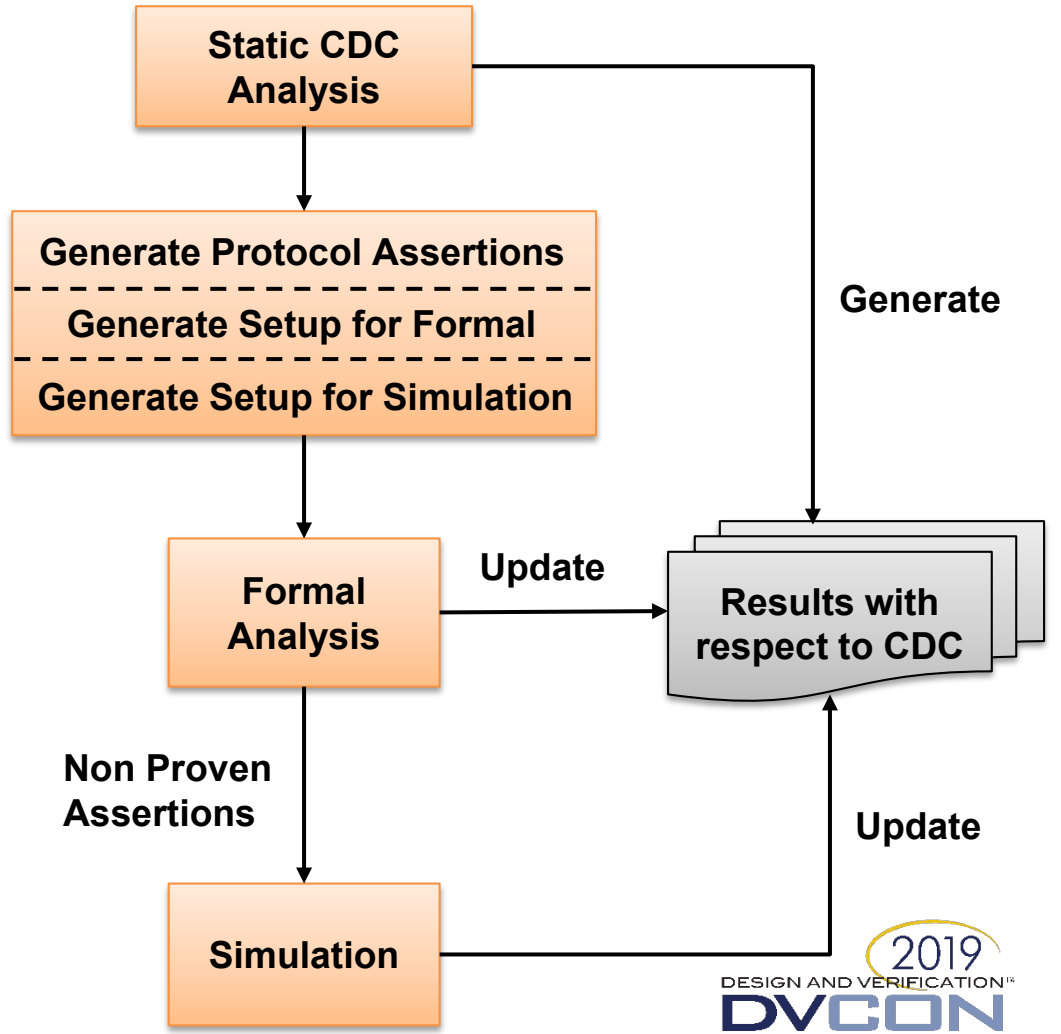

**Waveforms have no correlation to CDC-paths**
**Need both views (CDC-path & waveform)**

# Challenges with Existing Methodology

- Setup design for Formal, Simulation
  - Effort, time for translating CDC design setup to both environments
- Debug effort to review firings in Formal, Simulation
  - Technical expertise of both environments
  - Setup translation errors cause false violations
- Correlating assertions results in CDC vs. Formal vs. Simulation
  - Coverage, review of CDCs is cumbersome for complex crossings
- No re-utilization of benefits, efforts of Formal, Simulation
  - Simulation: More intuitive to understand but coverage issues
  - Formal: Offers exhaustive proofs but capacity, constraint issues
  - Formal proven assertions revalidated in Simulation

# Proposed Verification Methodology

- Perform static CDC analysis
- Generate:
  - Assertions for synchronizer protocols
  - Setup for Formal
  - Setup for Simulation
- Validate assertions in formal
  - Formal analysis using generated setup
- Validate assertions in simulation
  - Simulate design using generated setup
  - Only formal non-proven assertions



# Verification Methodology

- Automated design setup for Formal & Simulation
  - Static analysis setup exported to formal constraints
- Reduced formal firing debug effort
  - Avoid debug of unconstrained formal firings
  - Promote non-proven assertions to simulation
- Formal & simulation results correlated to CDC paths
  - Improved review/debug of CDC paths & assertion/coverage results
  - Avoids manual aggregation/correlation of assertion results
- Leverage formal efforts in simulation
  - Prune formally proven assertions from simulation

# Correlated Results View

- Formal, Simulation results correlated to CDC
  - Enables faster review of CDC paths, coverage closure
  - No manual correlation of assertion results required

```
============================================================
CDC Protocol Results
============================================================

CDC ID                Protocol ID                          Formal Result   Simulation Result
------------------------------------------------------------------------------------------
handshake_7492        cdc_protocol.handshake_7492          Fired           Fired
bus_two_dff_1183      cdc_protocol.bus_two_dff_1183        Fired           Covered
handshake_5883        cdc_protocol.handshake_5883          Inconclusive    Uncovered
two_dff_19174         cdc_protocol.two_dff_19174           Inconclusive    Covered
bus_two_dff_4271      cdc_protocol.bus_two_dff_4271        Proven          -
fifo_2332             cdc_protocol.fifo_2332               Proven          -
two_dff_68078         cdc_protocol.two_dff_68078           Proven          -
```

**CDC** | **Protocol Assertion Generation** | **Formal** | **Simulation**

# Existing vs. New Methodology (Formal)

| CDC Protocol Verification with Formal | | | | | | |
|---|---|---|---|---|---|---|
| Design | Setup time | Assertions | | | Run Time | Formal Coverage* |
| | | Total | Failed | Proven | | |
| A | 1w 3d | 170 | 79 | 91 | 24s | 100% |
| B | 2w 2d | 800 | 304 | 437 | 5hrs | 92.60% |
| C | 5w 4d | 8552 | 5673 | 877 | 7hrs | 76.60% |

Reduction in setup time

Reduction in false firings

Coverage indicates actual scenario

| CDC Protocol Verification with Formal | | | | | | |
|---|---|---|---|---|---|---|
| Design | Setup time | Assertions | | | Run Time | Formal Coverage* |
| | | Total | Failed | Proven | | |
| A | 2d | 170 | 32 | 138 | 55s | 100% |
| B | 5d | 800 | 119 | 654 | 6hrs | 96.60% |
| C | 1w | 8552 | 1825 | 4907 | 10hrs | 78.70% |

* Formal Coverage = ((Failed Assertions + Proven Assertions) / Total Assertions) * 100

# Existing vs. New Methodology (Simulation)

| CDC Protocol Verification with Simulation | | | | | |
|---|---|---|---|---|---|
| Design | Setup time | Assertions | | Run Time | Simulation tool Coverage** |
| | | Total | Failed | | |
| A | 10min | 170 | 14 | 20min | 91.70% |
| B | 17min | 800 | 83 | 35min | 88.30% |
| C | 30min | 8552 | 127 | 1hr | 79.40% |

Reduction in setup time

Formal effort utilization

Coverage indicates actual scenario

| CDC Protocol Verification with Simulation (after Formal) | | | | | |
|---|---|---|---|---|---|
| Design | Setup time | Assertions | | Run Time | Simulation tool Coverage** |
| | | Total | Failed | | |
| A | 1min | 32 | 6 | 20min | 97.31% |
| B | 1min | 146 | 34 | 35min | 97.06% |
| C | 5min | 3645 | 76 | 1hr | 87.47% |

# Conclusion

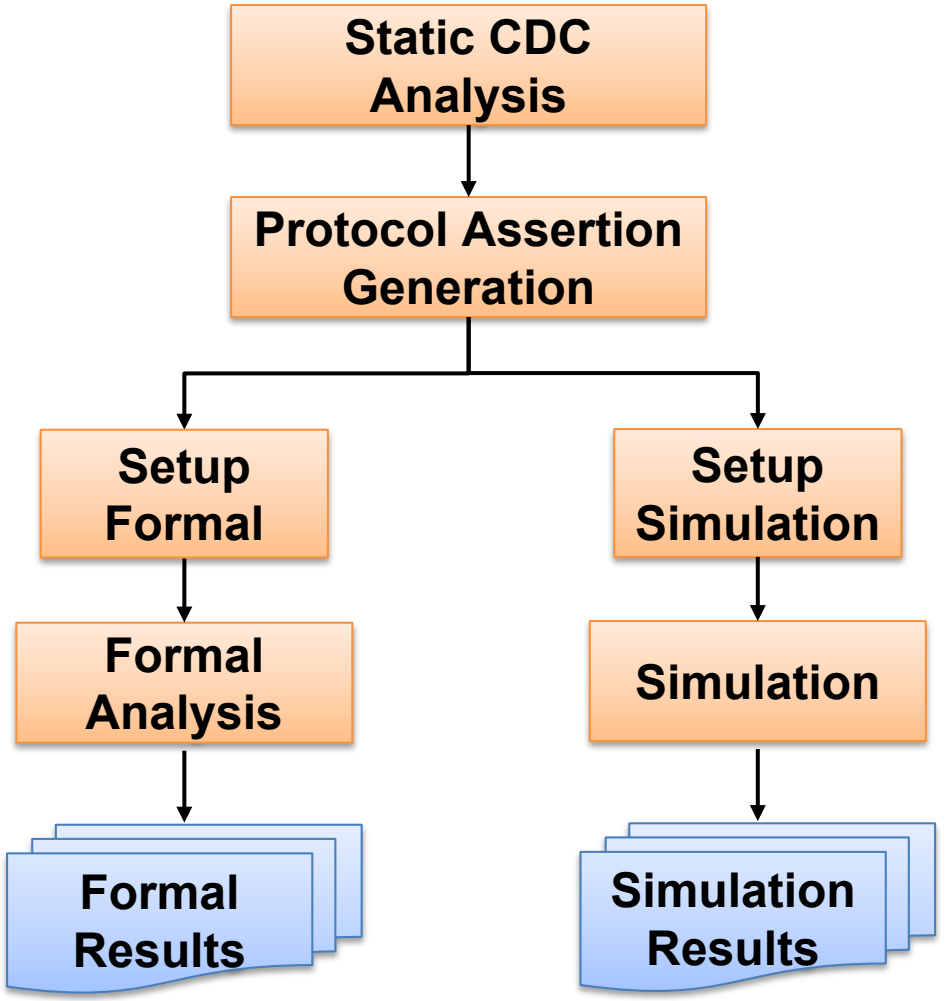
- Dynamic CDC Protocol Verification is critical
  - CDC bugs missed if synchronizer protocols not validated
- Proposed methodology helps achieve faster design closure
  - Seamless to adopt
  - Significant reduction in verification time, effort
  - Reduced chances of error thru automated setup generation
  - Overcomes challenges of Formal, Simulation methods
  - Enables efficient utilization of both methods

# Thank you!

# Questions?

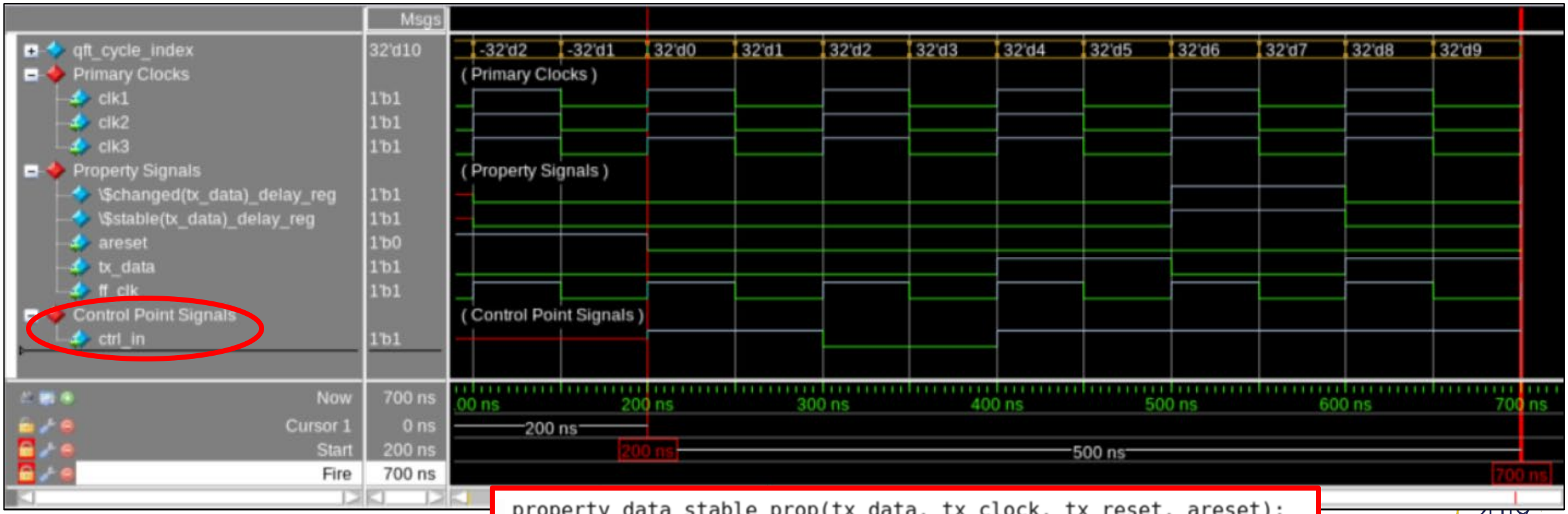
# Existing Verification Methodology

- Perform static CDC analysis
- Generate assertions for protocols of synchronizers
- Validate assertions in formal
  - Setup design for formal
  - Perform formal analysis
- Validate assertions in simulation
  - Setup design for simulation
  - Simulate design



# Setup, Debug Challenge (1)

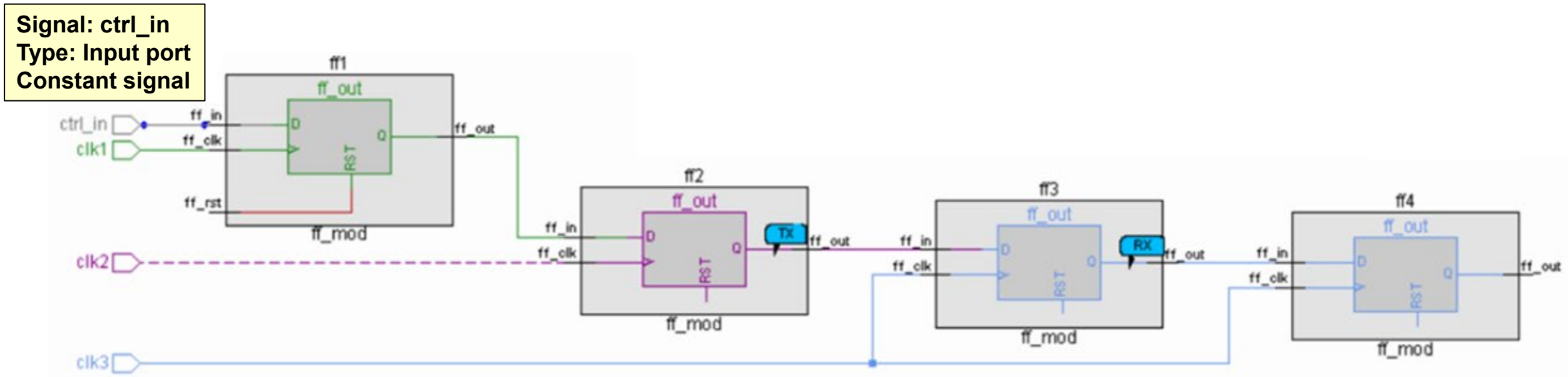
- Example: False two DFF synchronizer protocol firing in Formal
  - Data stability check firing due to change in value of **'ctrl_in'** signal




```
property data_stable_prop(tx_data, tx_clock, tx_reset, areset);
    @(posedge tx_clock) disable iff(areset)
  ##1 !tx_reset && $changed(tx_data) |=> $stable(tx_data)[*(1)];
endproperty
```

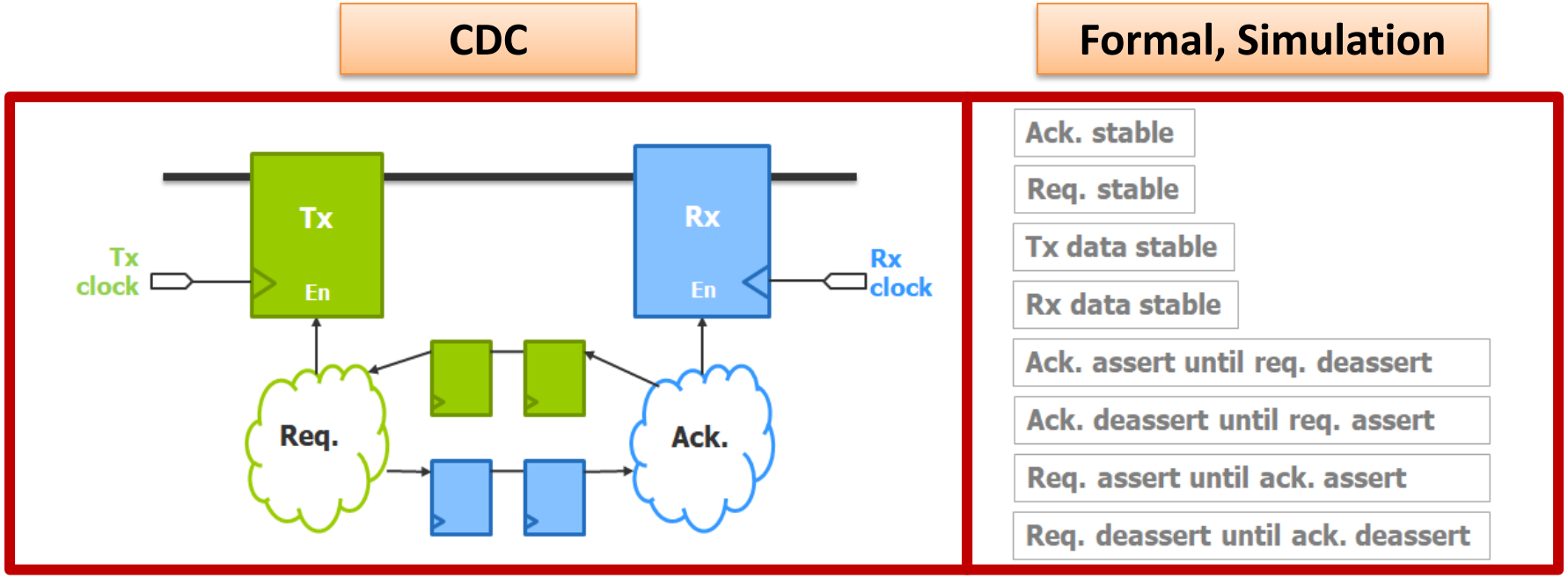
# Setup, Debug Challenge (2)

- False firing due to incomplete setup for Formal
  - Constraint specified on input signal **'ctrl_in'** during static CDC
  - Setup issue: Stable constraint missing from formal setup
  - Debug effort required for false firing caused due to incomplete setup



# Correlation Challenge

- Formal, Simulation environments very different from CDC
- Complex synchronizers have multiple assertions
  - Treated as separate entities in Formal, Simulation, but relate to a single CDC sync
  - Correlating results is cumbersome, time consuming
  - Errors during result correlation can lead to missed bugs




Multi-assertion Handshake synchronizer