

Accellera Verilog++ Extension assertion construct Requirements

Rev 1.4

December 28, 2001

Tom Fitzpatrick

fitz@co-design.com

Approved by Accellera HDL+ Assertions Committee on 12/20/01

1 Introduction

This document specifies the Accellera SystemVerilog extension assertion construct requirements. While establishing a set of requirements for the Verilog extension assertion constructs, the committee considered the following goals:

- *Expressiveness*: The extension assertion construct should be expressive enough to cover most implementation properties likely to be used by the design engineer.
- *Usability*: The extension assertion construct must be easy to understand and use by the design engineer.
- *Formalism*: The assertion language must have rigorous formal semantics to ensure correct compilation.

Extension assertion construct Justification: The question arises whether extension assertion constructs are necessary. After all, many Hardware Verification Languages (HVLs) provide powerful language features that can be used to describe correct temporal behavior. These HVLs can be used for data generation and results analysis thru temporal specification. In addition, the Accellera Formal Verification committee is actively defining a property specification language that can be leveraged by multiple verification processes. Therefore, some will say either HVLs or formal Property Languages *should* be able to provide all the power necessary to express assertions within the design. However, a variety of stakeholders in the design and verification flow necessitates a variety of approaches to specifying design properties.

The reality of the contemporary design and verification flow requires a broader look at the issues, and an understanding of the goals of the various stakeholders. The value white-box testing (through assertions) provides over a black-box testing approach has been validated by numerous sources. [Kantrowitz and Noack DAC 1996] [Taylor et. al. DAC 1998] [Bening and Foster Kluwer 2000] [Switzer et al. HDLCon 2000] [Foster and Coelho HDLCon 2001]. And, white-box testing can be performed with assertions, HVLs, or formal property languages. However, experience shows that verification engineers, whose goal is design validation, prefer an HVL approach to specifying properties of the design. On the other hand, the design engineers' focus is on implementation using hardware description languages (HDLs).

In addition to the dichotomy of goals, this issue also encompasses the areas of expertise of the various stakeholders. Quite often, the verification engineer lacks sufficient in-depth knowledge of design implementation details to provide effective white-box assertion coverage. On the other hand, during the course of RTL development, the design engineer makes low-level assumptions about the design's environment as well as other implementation assumptions. Experience has shown that if design assumptions or concerns are not captured during the process of RTL implementation, then many lower-level implementation properties are lost (that is, they will not be verified). For example, the *verification engineer* might wish to verify that a PCI bus controller exhibits correct behavior. This can be accomplished by using an HVL to generate correct bus functional stimulus and validate correct bus functional results. The verification engineer, however, would not validate specific implementation properties. Continuing with this example, assume that the PCI controller contains multiple embedded state machines. The *design engineer's* decision to implement a particular state machine as a one-hot versus some other type encoding is irrelevant to the verification engineer—provided that the PCI controller exhibits correct bus functional behavior. Yet, capturing properties of the implementation (for example, one-hot) during the design process provides better white-box coverage.

Ultimately, the most effective overall approach for capturing *implementation* properties is to include assertions as part of the HDL during RTL development. Assertions directly encoded within the HDL, versus maintained separately through HVLs or property languages, simplify the integration of reused blocks (that is, design reuse). Experience has shown that difficult forms of assertion specification limit the number of assertion capture during the implementation process—thus poorer quality of white-box coverage. Furthermore, revisiting the HDL after the implementation phase to add in assertions also results in a poorer quality of white-box coverage.

Hence, although there is some overlap in HDL assertion specification, versus HVL and Property Language specification, the end user of the particular form of specification is different. Thus, convenience of HDL assertion specification must be a consideration. This paper is intended to form a strawman proposal for assertion specification targeting the design engineer during Verilog implementation.

2 VHDL Assertions

Details on the VHDL assertion statement are included in this proposal to provide the reader with an example on how other HDLs have implemented a simple assertion mechanism.

VHDL provides a language construct for specifying a *static invariant* assertion in procedural code. For example:

```
[label] assert event
          [report message]
          [severity level]
```

The VHDL assertion statement checks that a specified condition (i.e., event) is true in a procedural fashion and reports an error if it is not.

The optional report clause specifies a message string to be included in error messages generated by the assertion. In the absence of a report clause for a given assertion, the string "Assertion violation" is the default value for the message string. The optional severity clause specifies a severity level associated with the assertion. In the absence of a severity clause for a given assertion, the default value of the severity level is ERROR.

Evaluation of an assertion statement consists of evaluation of the Boolean expression specifying the condition. If the expression results in the value FALSE, then an *assertion violation* is said to occur. When an assertion violation occurs, the report and severity clause expressions of the corresponding assertion, if preset, are evaluated. The specified message string and severity level (or corresponding default values, if not specified) are then used to construct an error message. The error message consists of at least:

- An indication that this message is from an assertion
- The value of the severity level
- The value of the message string
- The name of the design unit containing the assertion.

To express *temporal* assertion or *liveness* properties requires constructing finite state machines to trap the temporal behavior within the VHDL code. The action performed due to a given severity level is determined by the tool.

3 Assertion Language Requirements

3.1 Scope

While it is possible to create an assertion construct that will support both synchronous and asynchronous semantics, the first phase of effort will focus solely on synchronous assertions. This is to achieve the highest likelihood that today's existing formal verification and static analysis tools will be able to support the new assertion construct, since today's tools are limited to handling synchronous, or cycle-based, behaviors. At a later time, the committee or its successors may consider adding asynchronous assertions to the language.

3.2 Language Features

3.2.1 Assertion Identifier

The Verilog extension assert construct should have a unique identifier associated with it. Assertion identifiers are important for error reporting and upkeep within multiple verification tools.

3.2.2 Assertion Reset

The Verilog extension assertion construct should have a mechanism for preventing the assertion from firing. This reset mechanism will prevent the assertions from firing during verification and clear all state maintained by the assertion checker.

3.2.3 Assertion Sampling Clock

The Verilog extension assertion construct should have a mechanism for defining an optional sampling clock, which shall be a simple identifier or an expression, whose [raising/falling] edge defines the appropriate time to evaluate the `assertion` expression. If the sampling clock is supplied, the assertion expression will only be evaluated on the specified edge. If no sampling clock is specified then the assertion expression must be Boolean (non-sequential) and is evaluated immediately.

3.2.4 Assertion Expressions

The assertion construct shall evaluate an expression to determine if the assertion passes or fails. The expression may be any valid SystemVerilog expression.

Assertions are extremely useful for validating sequential behavior of designs, so there is a requirement for SystemVerilog to support **sequential expressions** to allow concise specification of sequences for evaluation in *an assertion*.

NOTE: *While it is likely that **sequential expressions** may be useful in other contexts within the language, the addition of sequential expressions as a separate language construct in SystemVerilog is beyond the scope of this document and may be considered in a future version of SystemVerilog.*

3.2.5 Assertion Severity Level

The Verilog extension assertion construct should provide a mechanism for defining the assertion violation severity level. The assertion committee might want to define various severity levels (e.g., ERROR, WARNING, NOTE, etc.). This could be accomplished using the Verilog attribute command.

Default simulation action for assertion failures of severity ERROR will issue a run-time message in simulation and halt the simulation. Assertion failures of severity WARNING will issue a run-time message in simulation, but the simulation will continue.

There is a need for SystemVerilog to support the specification of behaviors that do not directly correspond to ERROR or WARNING-level assertions. There are two alternatives being discussed:

1. Add another severity level to the proposed assertion construct, such as NOTE
2. Create a separate construct

Such behavior specifications are useful for coverage or reachability analysis.

3.2.6 Assertion Action

The Verilog extension assertion construct should enable the user to define an optional action associated with an assertion in simulation.

Instead of the default action on assertion failure, the user may specify an action to be executed when an assertion passes/completes and/or a possibly different action to be executed when the assertion fails. Any valid SystemVerilog statement, including a task call, shall be permitted as an assertion action.

3.2.7 Blocking and Nonblocking Assertions

The Verilog extension assertion construct should support both blocking and nonblocking assertions.

A blocking assertion will wait until the assertion completes (either passes or fails) before continuing execution with the next statement. A nonblocking assertion will “spawn” the evaluation of the assertion and continue executing the next statement. When the nonblocking assertion completes, the appropriate assertion action (if any) will be taken, according to the standard execution semantics of processes in SystemVerilog.

4 Usage Model

Assertions techniques should be applied during the following steps of design:

4.1 Specification Design Refinement

As a first step, an HDL assertion methodology must support a specification based top-down refinement process. In other words, prior to coding RTL, all interfaces between blocks (or between multiple engineers at a sub-block level) should be specified in a verifiable format (for example, a bus functional model combining FSMs and assertions). These interface assertions form verifiable contracts between design partitions, and are the key to successful integration of formal and semi-formal techniques at the block level of the design.

4.2 RTL Implementation

The next step involves coding assertions during the RTL implementation phase. Assertions directly coded within the HDL, versus maintained separately, simplify integration of reused blocks. Embedding the assertions directly in the RTL facilitates:

- linting (in a single step) the RTL source for syntactical errors related to assertion specification; and
- capturing design assumptions and knowledge at the point of development; which becomes a permanent record of the design intent, along with the RTL.

While verification has historically been delayed until completion of design testbench, coding assertions at the RTL implementation phase enhances [insert something about reliability or confidence]. Rather than delay verification until the point in time when multiple blocks can be integrated into a large model, block-level formal verification can begin prior to the completion of testbenches (or test vectors) using an assertion methodology. This important step enables the designer to identify lower-level implementation bugs, while exploring missing interface assertions (for example, constraints).

4.3 Design Reviews

Designer peer review is an important step in the development process. This enables the engineer to identify design misconceptions and receive peer feedback on corner case concerns. The quality of existing assertions should be reviewed during this step. In addition, missing assertions should be identified during the review process to ensure high-quality, white-box coverage.

4.4 Assertions and Simulation

During the simulation verification step, experience demonstrates that assertions coding within the HDL dramatically reduces the engineer's debug effort. Bugs identified in the course of simulation through means other than assertion

monitors indicate that the designer should add a new assertion that will trap this bug. This process addresses the following objectives:

- to capture the known corner case and document a permanent characteristic of the design;
- to provide the engineer with an increased awareness of how to code assertions; and
- to ensure (given the correct stimulus) that the bug can be identified in the original design, while providing a target to validate the modified design.

4.5 Hierarchical Formal Verification

Once the blocks have been verified and a reasonable confidence level has been achieved, hierarchical formal verification can be performed by applying assume/guarantee techniques that utilize block-level interface assertions. This process will identify design errors which cause interface inconsistencies amongst various blocks. This hierarchical process may be used, whether the block-level verification is done via simulation or via a formal tool. In formal verification, interface assertions provide constraints to the formal search engines during this step.

4.6 Semi-Formal Verification

Once the simulation environment stabilizes, semi-formal techniques can be introduced to enhance the stimulus-coverage quality. The interface assertions inserted in the design provide constraints to the formal search engine in this step.

4.7 Design Reuse

Verification is a central component of design reuse. Assertions embedded in the HDL reusable blocks validate proper design reuse integration. Furthermore, these assertions form a verifiable specification.

4.8 Functional Coverage Models

Capturing implementation level “function coverage” points is an important step in ensuring complete implementation validation. Assertions (with lower severity levels) are a mechanism that can be used by design engineer to specify important coverage points for verification. Having a similar technique for specifying design errors (assertions) and lower-level functional coverage points is desirable.