Catapult HLS User View Scheduling Rules

Stuart Swan, Platform Architect, Siemens EDA

8 January 2026

Introduction

In a high-level synthesis (HLS) design methodology, much of the benefit is lost if design verification and debugging must still be performed at the RTL level. In manual RTL design flows, RTL verification is typically one of the most costly and time-consuming phases of the overall flow. In HLS flows, RTL-level verification is even more challenging, because the RTL is machine-generated rather than hand-crafted.

This document presents a set of HLS scheduling rules, a modeling methodology, and a collection of formal proofs that together allow almost all design verification and debug for full systems to be carried out on the pre-HLS SystemC model. The methodology and proofs are organized around a latency-insensitive design style, while still fully supporting real-world techniques such as:

- latency-sensitive signal-level protocols
- latency-sensitive portions of systems
- both sequential and combinational logic
- pipelined designs
- shared memories between sequential processes
- reordering of RAM accesses to optimize hardware pipelines
- removal of pipeline registers for stable signal inputs to hardware pipelines

These techniques capture the requirements gathered from hundreds of Catapult HLS customer tape-outs and are needed to meet the demanding quality-of-results (QOR) targets traditionally achieved with manual RTL design.

The methodology presented here builds on established verification practices such as SystemVerilog UVM, constrained-random stimulus generation, and functional and code coverage. The system under test is modeled and verified in SystemC, and formal proofs establish behavioral equivalence for the synthesized RTL implementation.

Although the focus of this document is HLS, the design methodology and formal proofs can also be applied when HLS is not used, enabling much more efficient verification and debug at a higher level of abstraction than RTL.

A document abstract is provided in Appendix M.

Document Goals

This document presents HLS tool scheduling rules and modeling methodology rules. The goals are:

1. To provide easy-to-understand rules to HLS users.
2. To ensure precise and consistent rules in both SystemC and C++.
3. To offer rules that are effectively compatible with how Catapult currently operates.

4. To enable the best possible *quality of results* (QOR) in Catapult synthesis.
5. To cover all known user requirements and scenarios.
6. To serve as a suitable starting point for a standardization proposal (e.g., in Accellera SWG).

To illustrate the goals of this document more specifically, consider what an engineer writing a testbench for an HLS model needs to understand about how HLS tools operate. This engineer may be using SystemVerilog UVM or may be writing a testbench in C++/SystemC. They likely are not an expert in any specific HLS tool (and may not want to be), but their testbench needs to work for both the pre-HLS model as well as the post-HLS model. Thus, it is crucial for the DV engineer to have a precise understanding of how the HLS tool will transform the design while still enabling it to be fully verified. This document describes what transformations the HLS tool is allowed to perform so that the pre-HLS and post-HLS models can be effectively verified with the same testbench. The overarching philosophy of the scheduling rules is to present "no surprises" to such a DV engineer, while still giving the HLS tool ample freedom to optimize the design.

Background

HLS tools generate RTL from C++ models. Broadly speaking, this conversion takes a sequential C++ model and turns it into concurrent hardware that maintains the same behavior. HLS tools identify concurrent processes within the C++/SystemC model and then independently synthesize each process. Briefly, some of the techniques that HLS tools use to achieve good HW QOR when synthesizing each process include:

- Optimized scheduling based on the selected silicon target technology.
- Automatic HW pipeline construction according to the user's specifications.
- Automatic HW resource sharing.
- Automatic scheduling of memory accesses.

The internal behavior of each process is specified by the control and dataflow behavior of the C++ code within the process. However, the external communication that each process has with other processes and HW blocks is specified via IO operations that are coded within the model. To enable a reliable, scalable, and verifiable HLS flow that generates high quality hardware, the scheduling behavior of these IO operations needs to be precisely handled at all steps of the flow. This document specifies the rules that govern the scheduling behavior for these IO operations within HLS models. These rules are specified with respect to an individual process, but the intent of the rules is to enable reliable and verifiable behavior of large sets of interacting processes operating as a system in real-world designs. (Appendix G provides formal guarantees regarding the equivalence of the pre-HLS and post-HLS systems.)

By default, HLS tools can insert additional clock cycles (or latency) anywhere within a process -- for example, when pipelining a loop or to enable HW resource sharing. The overall approach used in this document is to make the entire design and testbench *latency insensitive* to the maximum extent possible, while still fully enabling key HW optimizations.

In some cases, designs or testbenches may use protocols which are latency sensitive. These situations can be handled by isolating the latency sensitive portions to small, self-contained parts of the design or

testbench, and then keeping the rest of the design and testbench latency insensitive. See Appendix D for more information.

In many cases the overall design will need to satisfy end-to-end latency requirements. For these designs it is still highly advantageous to use a latency-insensitive modeling approach and verify in the post-HLS model that the overall design latency requirements have been satisfied, since this is typically easy to do.

This document only covers sequential HW processes. Combinational HW processes are omitted since their synthesis is straightforward. All the examples and discussion in this document are for SystemC processes that are sensitive only to a single rising clock edge. (Appendix O discusses support for multiple clock domains.)

This document distinguishes between the following:

1. The *conceptual model* for the scheduling rules.
2. The simulation behavior of a model using the rules in C++ or SystemC.
3. The synthesis of a C++/SystemC model using the rules in an HLS tool such as Catapult.

The goal is to align each of these three cases as closely as possible, so that the user has easy to understand rules, while simulation and synthesis work without surprises. However, as we will see, there are practical considerations which may in certain cases cause small deviations from the conceptual model in either simulation or HLS.

A simple real-world example that illustrates the motivation for the scheduling rules is provided in appendix A of this document.

The examples referred to in this document are available here:

https://github.com/Stuart-Swan/Matchlib-Examples-Kit-For-Accellera-Synthesis-WG/tree/master

The most up-to-date version of this document is available here:

https://github.com/Stuart-Swan/Matchlib-Examples-Kit-For-Accellera-Synthesis-WG/blob/master/matchlib_examples/doc/catapult_user_view_scheduling_rules.pdf

An Analogy from RTL Synthesis

To better understand the specific purpose of this document, let's consider how RTL synthesis works. Say you have a sequential block that you are modeling in Verilog RTL, and it has an output port coded like:

```
Out1 <= #some_delay new_val;
```

In Verilog simulation, if some_delay is less than the clock period of the block, then it will probably not affect the overall cycle level behavior of the system during simulation. However, if some_delay is more than the clock period, it probably will.

During RTL synthesis, all RTL synthesis tools will ignore all delays in the input model, in this case even if some_delay is greater than the clock period. Some RTL synthesis tools might give a warning or error for the code above like "Simulation and synthesis results are likely to mismatch because the delay in model is greater than clock period." Some RTL synthesis tools might outright reject a model containing such delays.

One might argue that RTL synthesis tools should always match the Verilog simulation behavior of the input model. But the overall approach works well because RTL is a good and simple *conceptual model* that users and tool vendors can align around. The slight differences between the *simulation model* and the *conceptual model* used by RTL synthesis tools can be easily managed.

We'll return to this example later in this document.

Next let's clarify some terminology related to signal IO. Say you have a Verilog model like:

```
forever begin
  @(posedge clk);  // wait for 1st rising clock edge
  output1 <= input1 + 10;
  @(posedge clk);  // wait for 2nd rising clock edge
end
```

In this example we say that the read of the input1 signal occurs at the first wait statement, and the write of the output1 occurs at the second wait statement, since that is what you would observe in Verilog simulation when you ran this model. To generalize this, in Verilog designs within implicit state machines like this model which are only sensitive to a clock edge, signal reads occur at the closest preceding wait statement, and signal writes occur at the closest succeeding wait statement.

Catapult HLS Status Concerning Rules in this Document

A separate document provides a list of clarifications related to support within Catapult HLS for the rules described in this document. The items in the list are named *Cat#*, so that each item has a unique number.

This document annotates certain rules with *Cat#* to refer to the items in the separate document.

Terms Used in this Document

Latency-Insensitive: In digital hardware design, *latency-insensitive* refers to a system that operates correctly despite variable communication delays between components. This is achieved by using mechanisms to decouple computation from communication timing. Such designs improve scalability and reliability in complex systems with unpredictable or variable latencies. ARM's AXI4 and APB are examples of latency-insensitive protocols. ARM's AMBA 5 CHI credit-based NOC protocol is also an example of a latency-insensitive protocol.

Process: In Verilog, a process is an *always block* and its equivalent constructs. In SystemC, a process is an instance of an SC_THREAD or SC_METHOD.

Message-passing Interface: A *message-passing interface* reliably delivers messages (or transactions) from one process to another. This document uses this term to denote the type of communication found in Kahn Process Networks. See https://en.wikipedia.org/wiki/Kahn_process_networks
Message-passing read interfaces are always separate from message-passing write interfaces – there are no bidirectional message-passing interfaces. In this document, message-passing channels are assumed to be point-to-point: for each channel c, exactly one producer performs all Push_c operations and exactly one consumer performs all Pop_c operations.

Synchronization Interface: A *synchronization interface* synchronizes one process with another and/or with a global clock. For an example of a synchronization interface, see https://en.wikipedia.org/wiki/Barrier_(computer_science)

Signal IO: In digital HW design, signals are the fundamental communication mechanism. Signals enable communication between two HW blocks/processes, but communication with signals in real HW always incurs at least some delay because communication cannot be faster than the speed of light.
In HDLs and in SystemC, signal delays are modeled with the *delayed update* semantics.

blocking / non-blocking: A *blocking* message-passing interface suspends the execution of the calling process until the message is either sent or received. A *non-blocking* message-passing interface never suspends execution of the calling process: instead, a return code is provided to indicate whether the operation completed or not.

One-way / two-way handshake protocols: A one-way handshake protocol only has one signal between a sender and receiver to synchronize communication. A two-way handshake protocol has two signals (one in each direction) between a sender and receiver to synchronize communication.

shall: This term indicates that a compliant tool or flow is required to follow the indicated rule.

may: This term indicates that a compliant tool or flow is allowed to follow the indicated rule but is not required to do so.

Classes of Operations Involved in Scheduling Rules

There are three classes of operations involved in the scheduling rules:

1. Calls to message-passing interfaces (which are all ac_channel methods, all SystemC MIO calls except calls to SyncChannel)
2. Calls to synchronization interfaces (which are calls to ac_sync and Matchlib SyncChannel, also ac_wait and SystemC wait)
3. Signal IO (which are SystemC signal reads and writes, also C++ model *direct inputs*)

All the operations above are referred to as *IO operations*.

Basic Conceptual Model

The basic conceptual model encompasses processes that have no loop pipelining but may have preserved loops. If a process has a preserved loop, then the user may place a wait statement in the loop, or the HLS tool may automatically add one into the body of the loop. For a preserved loop the HLS tool may also add a wait statement at the loop termination. Such automatically added wait statements are called *implicit wait statements* in this document. Wait statements explicitly placed in the model are called *explicit wait statements* in this document.

Note that both *implicit wait statements* and *explicit wait statements* are classified as calls to a *synchronization interface*.

The basic conceptual model rules are:

1. Synchronization interface calls within a process always remain in the source code order.

2. Signal read operations occur at the closest preceding call to a synchronization interface. (Cat1)

3. Signal write operations occur at the closest succeeding call to a synchronization interface.

4. Message-passing operations are free to be reordered subject to the following constraints:
   - All message-passing operations before a call to a synchronization interface shall be committed before or in the same cycle in which the synchronization interface commits.
   - All message-passing operations after a call to a synchronization interface shall be issued after or in the same cycle in which the synchronization interface call commits.
   - Two message-passing operations on separate interfaces which appear in sequence in the model may be issued either in the same sequence or in parallel in simulation and in synthesis, but they shall not be issued in the reverse sequence. (Cat2)

Some explanation for the very last point: While pure message-passing systems with unbounded FIFOs are immune to reordering concerns, real-world hardware implementations have finite buffer sizes. Reversing the order of message-passing calls in a system with bounded FIFOs can introduce deadlocks that were not present in the original model. The last rule ensures that HLS tools cannot introduce such deadlock cases.

Pipelined Loops

When a loop is pipelined in HLS, the body of the loop is split into pipeline stages. HLS may start the next iteration of the loop before the current iteration has completed.

The user may place wait statements in the body of a pipelined loop to manually separate operations into their respective pipeline stages. Alternatively, the HLS tool may implicitly add these wait statements into the model to separate the pipeline stages. We call the former *explicit pipeline stage wait statements*, and the latter *implicit pipeline stage wait statements*.

Both explicit and implicit pipeline stage wait statements are classified as calls to a *synchronization interface*.

The scheduling rules for pipelined loops are the same as the rules given in the *basic conceptual model*, with the addition of these pipeline stage wait statements into the set of calls to synchronization interfaces. However, one rule from the conceptual model is relaxed when loops are pipelined: During loop pipelining, message-passing read operations from later loop iterations may be scheduled before or in parallel with message-passing write operations from the current loop iteration, and SystemC wait() statements and ac_wait statements, if present in the loop body, will not preclude this from occurring. Potential deadlocks are avoided by having the pipeline automatically flush. In this document, "automatic flush" means: if a required message-passing read (blocking Pop) is not available, the process blocks at that Pop exactly as in the unpipelined source; the implementation does not initiate any new message-passing Pops for younger overlapped iterations while blocked, and it does not withdraw any already-asserted blocking Push/Pop request. During the flush/drain phase, the implementation may continue to advance and complete already-started older work and may commit any resulting output Pushes until the pipeline is drained. See Appendix B for further discussion.

Example (II=1, latency=4, automatic flush): a loop that performs one blocking Pop and one blocking Push per iteration in the source may, after pipelining, commit four Pops before the first Push commits (pipeline fill). If a required Pop message is not available, the Pop blocks; the pipeline automatically flushes/drains overlapped younger iterations in a drain-only manner: it does not deassert any already-asserted blocking request, and it does not initiate any new message-passing Pops while blocked. The flush/drain phase may only complete already-started older work and commit any resulting output Pushes until the pipeline is drained. Under this discipline, the process's externally relevant blocking behavior matches the unpipelined source (it blocks as if no pipelining were present).

When HLS pipelines a loop, multiple iterations of the loop are overlapped and execute at the same time. During loop pipelining, for all IO operations, HLS shall ensure that an access to a specific message-passing interface, signal, or synchronization interface shall not be moved over or in parallel with an access to the same interface from a different loop iteration.

When HLS pipelining occurs, any signal reads and writes and associated synchronization interface calls become embedded in specific pipeline stages. With pipelining, the post-HLS model may begin execution of the next loop iteration before the current iteration has completed. Considering the entire set of signals read or written by the process, if HLS pipelining would cause the order of signal IO to differ between the pre-HLS and post-HLS models, or if any two signal IO operations that occur on the same clock edge in the pre-HLS model would not occur on the same clock edge in the post-HLS model, then the HLS tool shall detect such a situation and require the user to explicitly indicate in the model source (e.g., via a pragma) that HLS pipelining can still be used. (Cat7) Another way to state this requirement is the following: If a process communicates with other processes using only latency-insensitive protocols, then HLS pipelining by default shall not break any of the protocols.

Direct Inputs

Normal SystemC signal read operations occur at the closest preceding synchronization interface call (e.g., wait statement) in both the pre-HLS and post-HLS models. (Cat1). If the HLS tool adds states to the process, or if it pipelines the process, then this implies that the HLS tool must add registers for each such read operation such that the read occurs where specified in the pre-HLS model, and the value is stored until the point where it is consumed in the post-HLS model. The area cost of such registers may be high

if there are a lot of signals, and in some cases, it may be unneeded area since the value of the signals may not actually need to be stored internally to the process.

The simplest case is if such external signals are held stable after the process comes out of reset. In this case, HLS may assume that it is free to read the signal values as late as possible, with no need for register storage. This case is handled with the following pragma on SystemC signals and ports (Cat6):

#pragma hls_direct_input

To ensure that there are no pre-HLS versus post-HLS simulation mismatches, the environment that drives the signal shall hold it stable after all receiving processes that use this signal with this pragma come out of reset. Note that with this approach it is allowable to have *dynamic resets*, i.e. activation of block resets and associated resetting of direct input signals as part of the normal operation of the HW.

A related but somewhat more complex case is where input signals to the HW block may only be changed at "agreed upon" times, typically while the portion of the HW block that relies on them is temporarily idle. For example, a block may process 2D images. At the start of each new image, it may be desirable for the TB or external environment to update the control signals for how the block will process the next image. This needs to be done precisely since typically HLS designs are pipelined, and the HW pipeline for the current iteration must be fully *ramped down* before the input signals can be updated to affect the next iteration. In this case we can use the SystemC *SyncChannel* or C++ *ac_sync* primitives to precisely synchronize the DUT with the TB/environment to enable the input signals to be updated at the correct time. The `#pragma hls_direct_input_sync` directive shown below associates the sync operation with the direct inputs that it controls. The precise synchronization scheme shown here ensures that there are no pre-HLS versus post-HLS simulation mismatches even though we are using direct inputs and also changing their values while the design is executing.

```
  // This is example 61* in Catapult Matchlib examples
  sc_in<bool> SC_NAMED(clk);
  sc_in<bool> SC_NAMED(rst_bar);

  Connections::Out<uint32_t>  SC_NAMED(out1);
  Connections::In<uint32_t>   sample_in[num_samples];
  Connections::SyncIn         SC_NAMED(sync_in);
#pragma hls_direct_input
  sc_in<uint32_t> direct_inputs[num_direct_inputs];


  void main() {
    out1.Reset();
    sync_in.Reset();

#pragma hls_unroll yes
    for (int i=0; i < num_samples; i++) {
      sample_in[i].Reset();
    }

    wait();  // reset state

    while (1) {
#pragma hls_direct_input_sync all
     sync_in.sync_in();

#pragma hls_pipeline_init_interval 1
```

```
#pragma hls_stall_mode flush
     for (uint32_t x=0; x < direct_inputs[0]; x++) {
       for (uint32_t y=0; y < direct_inputs[1]; y++) {
        uint32_t sum = 0;
#pragma hls_unroll yes
        for (uint32_t s=0; s < num_samples; s++) {
           sum += sample_in[s].Pop() * direct_inputs[2 + s];
        }
        ac_int<32, false> ac_sum = sum;
        ac_int<32, false> sqrt = 0;
        ac_math::ac_sqrt(ac_sum, sqrt);  // internal loop unrolled in cat .tcl file
        if (sqrt > direct_inputs[7])
          out1.Push(sqrt);
       }
     }
    }
  }
};
```

From the perspective of the testbench or the environment, the updating of the signals controlled by the `hls_direct_input_sync` directive shall only occur at a precise point. The TB shall first wait for the `rdy` signal for the sync to be asserted by the DUT, and then the TB shall update all the input signals it wishes to change while simultaneously driving the sync `vld` signal high for one cycle.

It is important to note that the only safe operation to use to synchronize the updating of direct inputs is the sync operation as shown above. Other operations such as Push/Pop or ac_channel operations should not be used for this.

In the example above the DUT block that is being synthesized determines when to call sync, and thus it determines when the direct inputs will be updated. In some cases, it may be necessary for the environment around the DUT to determine when the direct inputs should be updated. In this case the same approach as shown above should be used, however a separate input from the environment to the DUT (either using a signal or a message-passing interface) should request that the DUT call sync as soon as feasible. This will ensure that the DUT has properly ramped down its pipeline and is ready to receive the newly updated direct inputs as per the overall synchronization scheme described above.

Additional Options for Scheduling Message-passing Interfaces

The following option may be added during HLS (Cat2):

```
STRICT_IO_SCHEDULING=relaxed
```

when this is specified, the HLS tool is allowed to reorder message-passing interface calls freely. However, it is still not allowed to move these calls across synchronization interface calls.

It is recommended that this relaxed option only be used when the user wants to see what order the HLS tool prefers to schedule message-passing interface calls (e.g., to achieve best QOR). Once the user knows the preferred order, it is recommended that the user modify the pre-HLS source code to reflect the preferred order, and then return to the use of the default scheduling modes. This methodology ensures that HLS cannot introduce any new deadlocks into the system as described earlier.

Scheduling of Array Accesses

Arrays may appear in HLS models, and they may be preserved through synthesis and mapped to RAMs. Pointers may also appear in HLS models, and pointer dereferences are resolved to array accesses during HLS.

There are two cases to consider for arrays for the purposes of the scheduling rules:

1. Array instantiation in the HW is internal to the process
   - The array accesses are not visible external to the process, and thus their scheduling is also not visible externally.
   - All the scheduling rules described elsewhere in this document remain unaffected in this case.

2. Array instantiation in the HW is external to the process
   - In this case the user model shall indicate how array accesses are mapped onto IO operations that are external to the process.
   - We call this the *array access mapping layer*. The *array access mapping layer* maps array accesses onto IO operations described above (signal IO, message-passing interface calls, and synchronization calls).
   - The user model may indicate that it is allowable for HLS to transform array accesses, for example, to cache, merge, split, or reorder array accesses (e.g., to improve QOR). These transformed operations, if allowed, are an outcome from the use of the *array access mapping layer*.
   - In all cases the scheduling rules described elsewhere in this document for the core IO operations (signal IO, message-passing calls, synchronization calls) remain unaffected.
   - In all cases array accesses shall remain constrained by any explicit synchronization interface calls present in the process in the source model. Precisely speaking, all array reads or writes before a synchronization call shall commit before or in the same cycle at which the synchronization call commits, and all array reads or writes after a synchronization call shall commit in a cycle after the synchronization call commits.
   - Note that if transformed operations occur and array accesses are visible externally in both pre-HLS and post-HLS model, then comparison of pre-HLS and post-HLS behaviors may need to account for the transformed operations.

When a loop is pipelined, multiple iterations of the loop are overlapped and execute at the same time. During loop pipelining, an access to a memory interface (or array) may be moved over or in parallel with an access to the same memory if the HLS tool can prove the reordering is conflict free. If the array/memory is external to the process, the *array access mapping layer* shall indicate that such reordering is allowable if such reordering is to occur during loop pipelining.

Additional States Added by HLS Synthesis

By default, HLS synthesis tools may add additional states to processes (e.g. add latency to enable resource sharing), which may introduce latency differences in the interface behavior between the pre-HLS and post-HLS models. These additional states are never included in the set of *synchronization interface calls* as described above.

When the directive IMPLICIT_FSM=true is set on a process, the HLS synthesis tool shall ensure that the cycle level behavior of the interfaces of the pre-HLS and post-HLS models shall be identical. With this option, the internal state machines of the pre-HLS and post-HLS models will be the same.

When the directive IO_MODE=FIXED is set on a process, the HLS synthesis tool shall ensure that the cycle level behavior of the interfaces of the pre-HLS and post-HLS models shall be identical. With this option, it is still possible that the state machine internal to the process is different between the pre-HLS and post-HLS models (e.g. the post-HLS model may choose to use a pipelined multiplier where the pre-HLS model did not.)

Avoiding Pre-HLS and Post-HLS Simulation Mismatches

The scheduling rules described in this document are designed to be easy to understand, while providing good QOR via HLS and generally avoiding any mismatches between the pre-HLS and post-HLS simulation behaviors.

Non-blocking message-passing operations (PushNB/PopNB in SystemC, C++ ac_channel nb_read/nb_write) are a potential source of mismatches between pre-HLS and post-HLS simulations since their behavior is inherently dependent on the latency within the model, which often changes during HLS. Because of this, non-blocking message-passing interfaces should only be used when no alternative approach is possible. For example, non-blocking message-passing interfaces are required to model time-based arbitration of multiple message streams which access a shared resource. A full discussion of recommended guidelines on the use and verification of non-blocking message-passing interfaces is provided in Appendix L. Note that the scheduling rules described previously in this document fully specify how HLS tools are required to schedule such operations.

Unidirectional message-passing between two processes should not be relied on to achieve synchronization between the two processes, since in general the message latency and storage capacity between the processes may be variable. Also, it is possible that the prefetch behavior of the message reader may vary. Bidirectional message-passing can be relied upon for synchronization between two processes. (An example of this is the AXI4 ar and r, and aw and b, channels). Note that such synchronization is weaker than explicit synchronization like SyncChannel or signal IO that uses a two-way handshake.

SystemC signal IO operations are a potential source of pre-HLS versus post-HLS simulation mismatches since timing behaviors may change between the two models. The following section provides guidance and rules to help avoid potential mismatches due to signal IO.

When signal IO operations are synchronized with a wait statement, there generally should be a proper two-way handshake associated with the wait statement so that the signal IO is latency insensitive. (Note that this statement does not apply to the signal synchronization approaches described in the Direct Inputs section.)

For example, here's a simple two-way handshake protocol when writing the signal `out_dat`:

```
out_dat = value;
out_vld = 1;
do {
```

```
      wait();
    } while (out_rdy != 1);
    out_vld = 0;
```

And here's a two-way handshake example when reading signal `in_dat`:

```
    in_rdy = 1;
    do {
      wait();
    } while (in_vld != 1);
    value = in_dat;
    in_rdy = 0;
```

Some signal-level protocols have different two-way handshaking approaches (e.g. ARM APB), but they are still latency insensitive.

If signal IO operations are associated with a wait statement and that wait statement does not have a proper two-way handshake, then the signal IO is likely to be latency sensitive and may result in pre-HLS versus post-HLS simulation mismatches. In some systems a one-way signal handshake is sufficient for reliable system operation. See Appendix E for further discussion.

The scheduling rules state that signal IO operations occur at either SystemC wait statements or SyncChannel calls (sync_in and sync_out). In the remainder of this section, we will use *wait* statement to refer to both.

RULE 1: It is always best coding style to group signal write operations just before their corresponding wait statement, and signal read operations just after their corresponding wait statement. (Cat3). An example is below:

```
 sc_in<int> i1;
 sc_in<bool> go;
 sc_out<int> o1;
 void my_thread() {
   int new_val=0;
   while (1) {
     o1.write(new_val);
     do {
       wait();
     } while (!go.read());
     new_val = i1.read();
     new_val = some_function(new_val); // function has no internal IO
   }
}
```

By placing the signal IO operations as close as possible to their corresponding wait statement, the HW intent is very clear. And there is no benefit either in terms of simulation performance or HLS QOR if they are placed further away from their corresponding wait statement.

Let's look at another similar example, which now also uses a Matchlib Connections blocking Pop operation:

```
 sc_in<int> i1;
 sc_in<bool> go;
 sc_out<int> o1;
```

```
 Connections::In<int> pop1;
 void my_thread() {
   int new_val=0;
   while (1) {
     o1.write(new_val);
     do {
       wait();
     } while (!go.read());
     int pop_val = pop1.Pop();
     new_val = i1.read();
     new_val = some_function(new_val + pop_val); // function has no internal IO
   }
}
```

According to the *Conceptual Model scheduling rules* part of this document, the Pop operation does not affect the scheduling of the i1.read() operation. However, it is possible that in the pre-HLS SystemC simulation, the Pop operation may block for a clock cycle or more (only if no items are available to Pop). This means that it is possible in the pre-HLS simulation that the value of the signal i1 may change between the time before the Pop operation starts and the time it completes. If this occurs, there may be a pre-HLS and post-HLS simulation mismatch if the HLS tool schedules the i1.read() operation at the wait statement. The proper fix to this issue (to reiterate) is to move the i1.read() operation as close as possible to its corresponding wait statement. This will make the potential simulation mismatch disappear, and it will not affect QOR or simulation performance.

To automatically avoid all such potential pre-HLS versus post-HLS simulation mismatches, HLS tools may provide error or warning messages in cases where models have the pattern shown above. Precisely speaking: if a blocking message-passing operation separates a signal read or write operation from its corresponding synchronization interface call, then the HLS tool may emit an error or warning indicating that reordering the signal IO operation and the message-passing operation in the source text is advisable.

Another scenario in which RULE 1 applies is shown below:

```
 sc_in<bool> go;
 sc_out<int> o1;
 void my_thread() {

   while (1) {
     wait();              WAIT 1
     o1.write(some_value);
     if (go.read()) {
       some_value = some_function();
     }
     else {
       wait();            WAIT 2
     }
     some_other_function();
     wait();              WAIT 3
   }
}
```

The signal read of `go` is clearly and uniquely associated with WAIT 1. However, the signal write of `o1` associates with WAIT 2 if `go` is false and WAIT 3 if it is not. This is a violation of RULE 1 and should be flagged as an error during HLS. The fix, as before, is to move the signal IO operation as close as possible to its intended wait statement so that the association is unconditional.

Next, let's consider *rolled* (or *preserved*) loops that perform signal IO within the loop body. Consider the following example:

```
 sc_in<int> i1;
 sc_out<int> o1;
 void my_thread() {
     wait(); // reset state
     while (1) {
       wait(); // start of while loop
       #pragma hls_unroll no
       for (int i=0; i < 10; i++) {
         o1.write(i1.read() * i);
       }
   }
}
```

Note that the `i1.read()` operation is located inside the `for` loop, so presumably the user's intent is that it should be read as the loop iterates. *If that is not the user's intent, then he simply should move the i1.read() operation before the loop start.*

In the post-HLS simulation, each iteration of the loop will consume at least one clock cycle, and a new value for i1 will be read (and a new value for o1 written) on each iteration. Again, this is the user's intent as per the code.

In the pre-HLS simulation, the for loop body will execute in zero time, and only the last write to o1 will have any effect. The solution to avoid this mismatch is to manually place a `wait()` statement within the for loop body so that the signal IO synchronization is explicit in the pre-HLS simulation.

RULE 2: If you have signal IO operations within *rolled* (or *preserved* loops), manually place a wait statement within the body of the loop to avoid pre-HLS versus post-HLS simulation mismatches, and while doing so also follow RULE 1.

To automatically prevent these types of pre-HLS versus post-HLS simulation mismatches, HLS tools may emit warning or error messages if they encounter a rolled loop which has signal IO operations within the loop body, and the loop body does not have a wait statement included within the loop body. (Cat4)

If a pre-HLS model adheres to RULE 1 and RULE 2, then all signal IO in the post-HLS model shall occur only at clock cycles that correspond to explicit wait statements or explicit synchronization statements. User designs that do not adhere to both RULE 1 and RULE 2 are *ill-formed*.

Returning to the Analogy from RTL Synthesis

At the beginning of this document, we presented the example of a Verilog sequential block with an output coded like:

```
Out1 <= #some_delay new_val;
```

Recall that in Verilog simulation, if some_delay is less than the clock period of the block, then it will probably not affect the overall cycle level behavior of the system during simulation. However, if some_delay is more than the clock period, it probably will.

During RTL synthesis, all RTL synthesis tools will ignore all delays in the input model, in this case even if some_delay is greater than the clock period. Some RTL synthesis tools might give a warning for the code above like "Simulation and synthesis results are likely to mismatch because delay in model is greater than clock period."

HLS tools that choose to adhere very closely to the *conceptual model* presented in this document should automatically provide errors or warnings for violations of RULE 1 and RULE 2 as described in the section above. This is analogous to the error message that the RTL synthesis tool would provide in the example directly above.

However, it is possible also that HLS synthesis tools may choose to adhere in these cases more closely to the pre-HLS SystemC simulation behavior. In this case such HLS tools might not provide any errors or warnings for violations of RULE 1 and RULE 2. This is analogous to an RTL synthesis tool being very smart (maybe even too smart) about synthesizing matching HW based on the actual value of some_delay in the example directly above.

Summary

At the beginning of this document, we said that the intent was to present "no surprises" to a DV engineer who is using a single testbench to verify both the pre-HLS and post-HLS models. The key aspects of the document which support this are:

- Three groups of IO operations are defined (message-passing, signal IO, and synchronization calls) and each is treated uniformly. These IO operations are easy for verification engineers to understand because they are already using them in their testbenches.

- The document specifically avoids complex constructs such as *protocol regions* used in some HLS tools.

- The document preserves the ability of the pre-HLS SystemC model to be *throughput accurate* by using a library such as Matchlib.

- Synchronization calls can affect the scheduling of signal IO operations, and synchronization calls can affect the scheduling of message-passing calls, but message-passing calls cannot affect the scheduling of signal IO operations and vice-versa.

- HLS cannot by default reverse the order of message-passing calls, so it cannot introduce new deadlocks into the post-HLS model.

- HLS pipelining is largely a *don't care* from the perspective of the verification engineer. If the design and the testbench are insensitive to changes in latency, and if external array accesses are not reordered or rearranged during loop pipelining, then the possible use of HLS pipelining will

not affect verification, provided the pipelines flush automatically. Even if the design or testbench are sensitive to changes in latency, or if they are sensitive to reordering or rearranging of external memory accesses due to the use of HLS loop pipelining, then the behavior of the DUT will only change in expected (rather than unexpected) ways. (Appendix G provides formal guarantees regarding the equivalence of the pre-HLS and post-HLS systems.)

- Signal IO operations in the post-HLS model by default always occur exactly at synchronization points (e.g., wait statements) that are either explicit in the pre-HLS model or easily deducible based on the use of loop roll/unroll or loop pipelining directives. The HLS tool can check that every signal IO operation is tightly coupled with exactly one wait statement / synchronization operation in the pre-HLS model.

Appendix A – Factory Analogy

The scheduling rules described in this document apply to pre-HLS and post-HLS HW models. Although the rules may seem abstract and perhaps even arbitrary, they are shaped by the need to model systems in the real world that are required to have predictable behavior.

To understand the motivation behind the rules, it might be helpful to draw a simple real-world analogy and its correspondence to the rules described earlier.

Consider a factory that produces various types of wooden furniture:

The factory consists of people (processes) stationed at workbenches with various tools.

Each person is given written instructions about the specific tasks they are to perform (C++ code within a process).

People are instructed to send or receive objects (messages) to or from other people in the factory.

Sending or receiving objects may be blocking or non-blocking from the perspective of a person.

There is a clock with a second hand on the factory wall that everyone can see. (HW clock).

People have colored flags they can raise or lower to communicate with other people (signals).

If someone raises or lowers a flag, this is only seen by others the next time the clock second hand is at the top of the clock. (propagation delay of signals between sequential processes)

A person can choose to pipeline the tasks that they were assigned by hiring subordinates (pipeline stages) and having each one do a subtask. In general, this will improve the throughput for the tasks that the person was assigned.

It is possible for two people to explicitly synchronize their work by communicating via a synchronization protocol such as a barrier (synchronization).

It is possible to restart the work of some or all the people by raising a reset flag (HW resets).

Assume:

1. That the time that people take to complete their various tasks is in general variable, and similarly that the time that objects (messages) take to pass between people is in general variable.
2. That each person in general wants to complete their tasks as quickly and efficiently as possible.
3. That the factory needs to be able to make multiple types of furniture at the same time. For example, it might make chairs that need to be different colors or have different styles.

To reliably produce output, each person in the factory will need to adhere to rules like those described in this document.

Here's a sketch of a specific way the above example relates to the scheduling rules:

Person 1 sends chair seats and chair backs to Person 2. This is done with blocking operations, and there is no storage capacity between the people when the objects are sent. (This means that a Push operation cannot complete until the corresponding Pop operation is performed.) Assume that the fastest an object can be sent between people is 1 minute.

The written instructions that person 1 is given are:

```
while (1) {
 // internal processing code for seats and backs ...
 seats.Push(seat_object);
 backs.Push(back_object);
}
```

The written instructions that person 2 is given are:

```
while (1) {
 seat_object = seats.Pop();
 back_object = backs.Pop();
 // internal processing code for seats and backs ...
}
```

If both person 1 and person 2 choose to perform their tasks sequentially as written, then objects will be passed over time as:

```
            Person 1            Person 2
Minute 1:   seats.Push(seat1);
Minute 2:   backs.Push(back1);  seat1 = seats.Pop();
Minute 3:   seats.Push(seat2);  back1 = backs.Pop();
Minute 4:   backs.Push(back2);  seat2 = seats.Pop();
Minute 5:                       back2 = backs.Pop();
```

If both person 1 and person 2 choose to perform their IO operations in parallel, then objects will be passed over time as:

```
           Person 1                                Person 2
Minute 1:  seats.Push(seat1); backs.Push(back1);
Minute 2:  seats.Push(seat2); backs.Push(back2);   seat1 = seats.Pop(); back1 = backs.Pop();
Minute 3:                                          seat2 = seats.Pop(); back2 = backs.Pop();
```

If person 1 chooses to perform his IO operations in parallel, and person 2 chooses to perform his IO operations sequentially as written, then objects will be passed over time as:

```
            Person 1                                  Person 2
Minute 1:   seats.Push(seat1); backs.Push(back1);
Minute 2:                                             seat1 = seats.Pop();
Minute 3:   seats.Push(seat2); backs.Push(back2);     back1 = backs.Pop();
Minute 4:                                             seat2 = seats.Pop();
Minute 5:                                             back2 = backs.Pop();
```

If person 1 chooses to perform his IO operations sequentially as written, but person 2 chooses to perform his IO operations sequentially in the reverse order as it was written, then objects will be passed over time as:

```
            Person 1             Person 2
Minute 1:   seats.Push(seat1);
Minute 2:   backs.Push(back1);   back1 = backs.Pop();
Minute 3:                        seat1 = seats.Pop();
```

In this case the person 1 seats.Push(seat1) operation at minute 1 will not complete at the start of minute 2. This means that the person 1 backs.Push(back1) operation will never start, and thus the Person 2 back1 backs.Pop() operation will never complete. So, the system will be in deadlock.

This example directly corresponds to the ordering rules related to message-passing operations in the *basic conceptual model* within this document, and in particular the specific rule that disallows reversing the order of message-passing operations.

Appendix B – Pipelined Loops and Message-passing

The scheduling rules state that during loop pipelining message-passing read operations from later loop iterations may be scheduled before or in parallel with message-passing write operations from the current loop iteration. This might seem to be in contradiction with the rules for message-passing operations described in the *basic conceptual model*. However, it is important to remember that each message-passing channel is *self-synchronized*. If a process has a pipelined loop that automatically flushes in the post-HLS model, then from an external perspective the only effect of allowing the message-passing read operations to occur earlier is like a *pre-fetch* operation. If the incoming message is not available, the pipelined process in the post-HLS model will flush, and its behavior from the external perspective will appear exactly as if it is not pipelined.

Appendix C – Verification of Designs that are Partially Latency Sensitive

This content has been moved to Appendix L.

Appendix D – Modeling Latency-Sensitive Protocols

In some cases, designs or testbenches may use protocols which are latency sensitive. These situations can be handled by isolating the latency-sensitive portions to small, self-contained parts, and then keeping the rest of the design and testbench latency insensitive.

Consider a case where a signal-level protocol is latency sensitive. The protocol will have specific timing behavior that it must meet. To handle this, we create a transactor that has two sides: the first side interacts with the signals and handles the detailed timing requirements, and the second side sends and receives messages with the rest of the system. The message-passing side is latency insensitive.

To properly model the detailed timing behavior, the transactor is modeled at the cycle-accurate level in SystemC. There is an example of such a transactor model in the following document and example:

https://github.com/Stuart-Swan/Matchlib-Examples-Kit-For-Accellera-Synthesis-WG/blob/master/matchlib_examples/examples/53_transactor_modeling/transactor_modeling.pdf

Appendix E – One-Way Handshake Protocols

In some systems a one-way signal handshake is sufficient for reliable system operation. When using a one-way handshake, the implicit assumption is that the "missing" handshake isn't required since it is always true.

For example, in time-domain signal processing hardware designs, signal processing HW blocks may input new samples at a fixed rate. The HW blocks are always ready to receive new samples on each clock, but they need to know if the samples are valid. These types of designs can be modeled with the one-way handshake dat/vld protocol demonstrated in this example:

https://github.com/Stuart-Swan/Matchlib-Examples-Kit-For-Accellera-Synthesis-WG/tree/master/matchlib_examples/examples/32_dat_vld

Appendix F – Scheduling Rules: Modeling Guidelines Summary

1) Prefer to use Connections::In/Out + SyncChannel over signal IO and wait().

2) Prefer to use Pop()/Push() over PopNB()/PushNB().

3) When pipelining a loop, prefer to use `hls_stall_mode flush`.

When using signal IO:

4) If modeling a cycle-accurate process, use `disable_spawn` and follow example 53_transactor_modeling style and do not use Push/Pop in the process.

5) If modeling a *direct input*, use `hls_direct_input` and possibly `hls_direct_input_sync`, and only change the signal at allowed times.

6) If combining signal IO with Connections::In/Out in same process, use proper signal IO handshake that does not rely on In/Out ports for process synchronization. Place signal IO operations very close to their wait() statements.

7) Unless you are modeling a cycle-accurate process, you should expect that latency will change between the pre-HLS and post-HLS models.

Appendix G – Equivalence Rules

This document informally states that a primary goal is to present "no surprises" to a DV engineer using the same testbench to verify the pre-HLS and post-HLS models.

Somewhat more formally, we can show how the scheduling rules within this document establish a set of equivalence rules between the pre-HLS and post-HLS models that provide strong guarantees about their behaviors.

The *basic conceptual model* establishes the base behavior for a single process:

1) Synchronization interface calls always remain in source code order.
2) Signal reads occur at closest preceding synchronization interface call.
3) Signal writes occur at closest succeeding synchronization interface call.
4) All message-passing operations before a call to a synchronization interface shall be committed before or in the same cycle in which the synchronization interface commits.
5) All message-passing operations after a call to a synchronization interface shall be issued after or in the same cycle in which the synchronization interface call commits.
6) Two message-passing operations on separate interfaces which appear in sequence in the model may be issued either in the same sequence or in parallel in simulation and in synthesis, but they shall not be issued in the reverse sequence. Operations on the same message-passing interface are issued in source order (they are never reversed).
7) Synchronization calls can affect the scheduling of signal IO operations, and synchronization calls can affect the scheduling of message-passing calls, but message-passing calls cannot affect the scheduling of signal IO operations and vice-versa.
8) The STRICT_IO_SCHEDULING=relaxed option is not used.
9) In the pre-HLS model, the storage capacity of message channels is zero (rendezvous-style communication).

Conceptually, systems are composed of many such processes which follow the basic conceptual model, and which communicate using only synchronization interface calls, latency-insensitive signal-level protocols, and committed message-passing transfers. If a design uses non-blocking message-passing calls (PushNB/PopNB), then unsuccessful polls are treated as internal ε-steps (no Σ-event), and each successful completion is represented in Σ as the corresponding committed Push_c/Pop_c transfer (Σ records transfers, not failed polls). If the resulting latency-sensitive behavior is externally visible at the DUT boundary, the snooping wrapper of Appendix L may be used to align the selected admissible pre-HLS execution with the RTL. Here we call this system of processes the *conceptual system*.

Practically, the modeling approach described above is too restrictive for real-world systems with optimized HW, so the scheduling rules in this document allow for key HW optimizations. But this is done

in a carefully controlled manner, such that the HW optimizations do not break equivalent behavior with the *conceptual system*.

Here is a summary of the HW optimizations that the scheduling rules allow, and a brief description of how we maintain equivalent behavior with the *conceptual system*:

1. Pipelined loops: Message-passing read operations from later loop iterations can execute before message write operations from the current loop iteration. Assuming the pipeline automatically flushes, this behavior change can be viewed as a *prefetch* operation. If the message to be read is unavailable, the pipeline will flush, and the process will appear exactly as if it is not pipelined.

2. Pipelined loops: HLS by default will not break any latency-insensitive signal IO protocols when pipelining loops.

3. Direct inputs: Signals that do not change after a process comes out of reset can be read as late as possible using *hls_direct_input*, saving register area.

4. Direct inputs: When *hls_direct_input_sync* is used, signals read by a process are updated at the precise point at which the HW pipeline is guaranteed to be ramped down, so the signal values do not need to be saved within pipeline registers, saving register area.

5. Memory accesses: HLS can reorder memory accesses within a process only if it can prove that the reordering is conflict-free.

6. Shared memories: Memories shared between processes are modeled as simple C arrays but always include explicit synchronization between processes in both the pre-HLS and post-HLS models.

7. Non-blocking message-passing interfaces: They are modeled at the level of committed transfers (successful completion), with unsuccessful polls treated as ε-steps and thus not part of Σ. If latency differences in these committed-transfer events are externally visible at the DUT boundary and must be aligned for verification, equivalent behavior between pre-HLS and post-HLS systems can be maintained by snooping the post-HLS system and using this to delay pre-HLS message arrival (Appendix L).

8. Latency-sensitive global signal IO: If latency differences are externally visible to the DUT, equivalent behavior between pre-HLS and post-HLS systems can be maintained by snooping the post-HLS system and using this to delay pre-HLS signals.

9. Latency-sensitive local signal IO: Isolate local latency-sensitive protocols to small, dedicated transactors, and use latency-insensitive signal IO or message-passing to communicate with the rest of the system.

10. One-way signal handshake protocols: Only use in cases where backpressure is not possible and embed assertions into the model to check that this is always true.

11. Combinational processes: If the pre-HLS model contains combinational processes, they will have identical behavior in the post-HLS model and thus they cannot introduce any differences between the models.

Taken as a whole, these rules allow full system verification to be performed on the pre-HLS system model. Full system verification does not need to be repeated on the post-HLS RTL system, provided the equivalence rules described above are followed.

Formalization of the Equivalence Rules in Appendix G

The following notation is used in this section.

Symbol Meaning

P	A process (thread or method) in the design
Σ	The alphabet of observable IO actions
τ_P	A (finite or infinite) per-cycle trace of observable actions executed by process P: for each global clock cycle t, τ_P[t] is the (possibly empty) set of Σ-actions committed by P at t. Actions committed in the same cycle are treated as simultaneous (unordered); only cross-cycle order (and the explicit E1–E5 constraints) is semantically significant. Single-op-per-cycle (channel endpoint) constraint: for each message-passing channel c and each clock cycle t, there is at most one committed Push_c event in the entire system at t, and at most one committed Pop_c event in the entire system at t (i.e., the producer endpoint is single-ported for Push_c and the consumer endpoint is single-ported for Pop_c). Thus, the only "same-cycle" multiplicity on a single channel is the (Push_c, Pop_c) pair of the same transfer (including rendezvous at B(c)=0).
S	The subset of Σ that are synchronization calls (explicit wait, SyncChannel, START_P/FINISH_P indicating process start/finish)
R	The subset of Σ that are signal reads
W	The subset of Σ that are signal writes
M	The subset of Σ that are message-passing calls (Push, Pop, etc.)

A *system trace* is the tuple
τ = (τ_P)_P, one component per process.
For any action a ∈ Σ, let clk(a) be the clock cycle at which a is *committed*.
For any message operation *m*, issue_pre(m) / issue_post(m) – is the clock cycle in which the pre-HLS or post-HLS process first asserts the ready/valid handshake request for *m*, independent of the later commit cycle clk_pre(m) / clk_post(m).
(No deassert-before-commit assumption.) For blocking message transfers (i.e., those that contribute committed Push_c/Pop_c events to Σ), once the request for *m* is asserted, it is not withdrawable: it remains asserted in every subsequent cycle until the corresponding transfer commits at clk_pre(m) / clk_post(m) (and for Push_c the payload remains stable while the request is outstanding). Because issue timing is under sole control of the issuing process, it can be used to express per-process ordering constraints.

---

1. Conceptual Model for a Single Process

For every process P the pre-HLS trace τ_P must satisfy the following *partial-order constraints*:
R1 (Program order of S).
∀ s1, s2 ∈ S : s1 <_src s2 ⇒ clk(s1) < clk(s2)
R2 (Location of R/W).
∀ r ∈ R : clk(r) = clk(pred_S(r))
∀ w ∈ W : clk(w) = clk(succ_S(w))
where pred_S(r) (resp. succ_S(w)) is the closest synchronization call that precedes (resp. follows) statement r in the augmented source order, where the augmentation includes any implicit wait / stage-wait synchronization calls introduced by tool directives (e.g., loop pipelining) as described in the main text; these implicit stage waits are members of S for purposes of pred_S/succ_S and the E-rules.
If no lexical predecessor (successor) exists, a virtual synchronization operation at time 0 (resp. ∞) is assumed.
R3 *(Isolation around S).*
Let pref_S(s) (resp. suff_S(s)) be the set of message calls lexically before (resp. after) synchronization call s. Then
∀ m ∈ pref_S(s) : clk(m) ≤ clk(s) and ∀ m ∈ suff_S(s) : issue_pre(m) >= clk(s).
R4 (Safe message issue ordering).
For every pair m1,m2 ∈ M within the same process,
m1 <_src m2 ⇒ issue_pre(m1) ≤ issue_pre(m2).
(For same-channel operations, this simply states that calls on a single interface are issued in program order; for distinct channels, it forbids issuing them in reverse order.)
Post-HLS obligation. The implementation must satisfy E3: preserve same-interface issue order, preserve the no-reverse rule for distinct interfaces except for the pipelined-loop read-ahead relaxation described in "Pipelined Loops," with deadlock concerns addressed by pipeline flush.
R5 (Channel capacity semantics; Sys vs. Sys_B).
Appendix G defines the rendezvous source model Sys, in which every channel has capacity 0.
Concretely: for every channel c and any clock cycle t, the number of unmatched committed Push_c actions is zero and the number of unmatched committed Pop_c actions is zero; equivalently, no Push_c shall commit unless a matching Pop_c also commits at t, and no Pop_c shall commit unless a matching Push_c also commits at t.
In Appendices I–K we additionally use the buffered source interpretation Sys_B: the same source processes as Sys, but interpreted under bounded-FIFO channel semantics with capacities B(c) matching RTL(Sys) (E4), with rendezvous recovered as the special case B(c)=0.

The source conceptual semantics for a process is thus a labeled partial order (Σ, ≤_P) generated by R1–R4 plus the channel semantics of Sys (rendezvous) or Sys_B (bounded FIFO), depending on which model is being referenced.

---

2. Equivalence Relation

Let τ_pre and τ_post be the Σ-traces (finite or infinite) of the same process before and after HLS, where each Σ-event is labeled exactly as in "Common Formal Definitions for Appendices I–K" (e.g., Push_c(v), Pop_c(v), Read(sig,val), Write(sig,val), and synchronization events).
Convention (augmented S): all references to S, pred_S/succ_S, and <_src in E1–E5 use the augmented source order of R2, including any implicit wait / stage-wait synchronization calls introduced by tool directives (e.g., pipelining). Thus τ_pre is taken from the source interpreted with those implicit stage waits included as Σ-visible synchronization events (members of S).
Σ-event matching convention. We use a canonical per-endpoint occurrence matching to make "the same Σ-events" precise. For each channel c, match committed Push_c and Pop_c events by their ordinal

occurrence on that channel (e.g., the k-th committed Push on c in τ_pre matches the k-th committed Push on c in τ_post; likewise for Pop_c). For each such matched pair, the endpoint (c) and the payload/value label must agree. For each observable signal sig, match Read(sig,·) and Write(sig,·) by their ordinal occurrence on that signal within the process trace, again requiring the value labels to agree. In forming τ_pre and τ_post, we apply the following canonicalization for observable signals: within each anchor interval between consecutive synchronization events in the augmented order S (including implicit stage-wait synchronizations), we record at most one Σ-visible Read(sig,val) and at most one Σ-visible Write(sig,val) for each (process, sig), with the anchor cycle given by E2. Any additional physical sampling of sig by the implementation, or redundant re-driving of sig within the same anchor interval, is treated as an internal ε-step and must not change the recorded value label. If a design intentionally relies on intra-interval changes of sig, or on distinguishing multiple reads/writes of sig within the same anchor interval, then sig must be modeled using an explicit synchronized interface (rather than as an ordinary observable signal) so that those distinctions become Σ-visible.
For synchronization events (including implicit stage-wait synchronizations from the augmented S), match by their per-process occurrence index in the augmented source order (R2).
Independent Σ-events on different endpoints (including distinct message-passing interfaces) may commute and/or be grouped differently within a clock cycle as permitted by the R-rules and E3. Accordingly, τ_pre and τ_post are not required to be identical as a single total order, nor to agree on same-cycle "grouping" of distinct-interface Push/Pop operations, beyond the explicit ordering/timestamp constraints in E1–E5 below.

We say τ_pre ≈ τ_post iff the two traces match on Σ in this sense, and all of the following hold:
E1 (Synchronization-order preservation).
$\forall\, s1,s2 \in S : clk\_pre(s1) < clk\_pre(s2) \Rightarrow clk\_post(s1) < clk\_post(s2)$
E2 (Signal-visibility preservation).
$\forall\, r \in R : clk\_post(r) = clk\_post(pred\_S(r))$
$\forall\, w \in W : clk\_post(w) = clk\_post(succ\_S(w))$
E3 (Safe message issue ordering; pipelined-loop read-ahead permitted).
For any two message operations m1,m2 ∈ M issued by the same process:
(i) Same-interface order is always preserved: if m1 and m2 access the same message-passing interface/channel and m1 <_src m2, then issue_post(m1) ≤ issue_post(m2).
(ii) Distinct-interface no-reverse holds except for pipelined-loop read-ahead: if m1 and m2 access distinct message-passing interfaces and appear in sequence in the source, then they shall not be issued in reverse order unless they are a pipelined-loop read-ahead case as described in "Pipelined Loops" (i.e., a message-passing read from a younger overlapped iteration issued before a message-passing write from an older iteration).
In that pipelined-loop read-ahead case, reverse issue order is permitted, and deadlock risks are addressed by the automatic flush discipline described in "Pipelined Loops" and Appendix K (drain-only: no withdrawal of asserted blocking requests; no flush-initiated message Pops).
E4 (Per-channel bounded-FIFO semantics).
For every observable channel c with capacity B(c), the projection of τ_post to events on c is FIFO-legal for that bound:
• No drop/duplicate + payload preservation: if the Push_c(v) events on c occur with payload sequence $v_1,v_2,\ldots$ then the Pop_c(v) events occur with payload sequence $v_1,v_2,\ldots$ (i.e., pops return the oldest unmatched pushed value).
• No overflow/underflow: for every cycle-aligned prefix π_t of the c-projection—i.e., π_t contains exactly the events on c committed in cycles < t—letting push(π_t) and pop(π_t) be the number of Push_c and Pop_c events in π_t, we have

$0 \le \text{push}(\pi\_t) - \text{pop}(\pi\_t) \le B(c)$.
Equivalently, the abstract occupancy after cycle t−1 is $\text{occ\_c}(t) = \text{push}(\pi\_t) - \text{pop}(\pi\_t)$.
(Rendezvous is the special case B(c)=0, which implies $\text{push}(\pi\_t)=\text{pop}(\pi\_t)$ for all t, allowing Push_c and Pop_c to commit in the same cycle without violating the bound.)
E5 *(Messages cannot cross syncs).*
For every message m and synchronization call s,
$\text{clk\_pre}(m) \le \text{clk\_pre}(s) \Rightarrow \text{clk\_post}(m) \le \text{clk\_post}(s)$
$\text{issue\_pre}(m) >= \text{clk\_pre}(s) \Rightarrow \text{issue\_post}(m) >= \text{clk\_post}(s)$

See *Appendix I – Per Process Trace Equivalence Proof* for formal proof of the following:
For any single source-level process P that obeys the conceptual R rules and B rules, when interpreted as part of Sys_B (i.e., bounded-FIFO channel semantics with finite capacities $B(c) \ge 0$ matching RTL(Sys)), every finite observable trace produced by P has a matching post-HLS RTL trace that satisfies E1–E5. The rendezvous Sys case is recovered by setting B(c)=0.

---

3. Allowed Transformations and Why They Preserve ≈

Transformation permitted by the rules	Formal justification
Loop pipelining (overlaps iterations)	Creates additional S actions (implicit stage waits), so R1–R5 (and hence E1–E5) are applied with the expanded S set. Loop pipelining may commute independent Σ-actions across iterations (e.g., across distinct channels), but it must still preserve: (i) per-channel FIFO legality (E4), (ii) the required issue discipline (E3) for source-ordered pairs, and (iii) the sync-boundary constraints (E1/E5) with respect to the (explicit + implicit) S-actions.
Re-ordering of message reads vs. later writes inside a pipeline	Allowed only when the two actions are on different channels and the pipeline auto-flushes. In that case, the transformation is only a commutation of independent actions: it preserves each channel's projection (and thus FIFO legality, E4), respects the source-order constraints that actually apply (E3), and does not move any message issue across a synchronization boundary (E5, with implicit stage waits treated as S-actions).
#pragma hls_direct_input (late sampling of static signals)	This pragma imposes a designer/environment stability contract: the signal's value must remain stable after reset (or after its last permitted update) while the receiving process may consume it. The logical signal Read actions r remain anchored exactly as in E2 ($\text{clk\_post}(r) = \text{clk\_post}(\text{pred\_S}(r))$). HLS may implement this by sampling the signal later (instead of inserting internal storage), but because the signal is stable the sampled value equals the value at pred_S(r); therefore E2 and ≈ are preserved.

Transformation permitted by the rules	Formal justification
#pragma hls_direct_input_sync (controlled updates)	This pragma imposes an explicit timing contract on the environment: the controlled direct-input signals may change only on the cycle of the designated synchronization call s* (i.e., during the sync handshake). With that contract, the logical anchoring required by E2 is preserved: for the receiving process, the relevant Reads are anchored at the closest preceding synchronization call pred_S(r) = s*, and any environment update Write w_update is aligned with synchronization (succ_S(w_update) = s*). HLS may still implement late sampling internally, but the value observed is the same as the value at the E2 anchor point, so ≈ is preserved without modifying E2. Instrumentation note (logical anchoring). In the Σ-traces used for ≈ checking, each signal Read/Write event is timestamped at its E2 anchor point (e.g., clk_post(pred_S(r)) for Reads), not at any later physical RTL sample cycle that HLS may introduce. Any internal late-sampling micro-steps are treated as ε-steps. Therefore, equivalence checking must instrument/record the logical Read/Write events at the anchor (or use a wrapper/transactor that exposes only those anchored events), rather than naively timestamping the physical sample.
Memory-access reordering proven conflict-free	Let addr(a) be the symbolic address of access a. If the tool proves $addr(a_1) \neq addr(a_2)$ for the overlapped window, then the commutation of a_1 and a_2 is observationally silent; no external signal/message depends on the internal order.
Implicit FSM states / added latency	Extra states introduce *silent* ε-steps between observable actions; the partial order on Σ is unchanged, so E1–E5 are unaffected.
Shared-memory arrays with explicit synchronization	When a memory is accessed by multiple processes, the *designer* explicitly coordinates access with a sync operation modeled as an S-action. Because these S-actions appear in both traces, the read/write order is fixed by E1–E2, port-level FIFO legality is preserved by E4, and the overall equivalence relation ≈ still holds.
Non-blocking message-passing (PushNB/PopNB) verified by post-HLS snooping	If the latency differences are externally visible to the DUT, a verification wrapper delays the pre-HLS side so that the committed transfer events (successful completions) occur in the same order/timing as observed on the post-HLS channel. This wrapper is itself purely synchronising (S), so it cannot violate R1–R5. Once the wrapper is assumed, τ_pre and τ_post coincide on the committed message-transfer history recorded in Σ (i.e., the Push_c/Pop_c commit events), so E3–E5 are preserved. Unsuccessful non-blocking polls remain ε-steps and are not required to match. This is not a

Transformation permitted by the rules	Formal justification
	transformation that inherently preserves ≈, but rather a verification technique to enforce equivalence for inherently latency-sensitive operations.
Latency-sensitive *global* signal IO matched by snooping	If the latency differences are externally visible to the DUT, the same "mirror-and-delay" wrapper used for NB channels is applied to any globally-visible signal whose timing matters. Because the wrapper inserts only S-actions, the partial-order constraints are unchanged. This is not a transformation that inherently preserves ≈, but rather a verification technique to enforce equivalence for inherently latency-sensitive operations.
Latency-sensitive *local* signal IO isolated in cycle-accurate transactors	Local timing-exact protocols are confined to dedicated transactor processes that expose only latency-insensitive M or S operations to the rest of the design. Since the transactor boundary is now the observable interface, R1–R5 apply *outside* the timing-sensitive region, so system-level ≈ still holds.
One-way signal-handshake protocols with run-time assertions	For single-direction vld or rdy signals, an assertion proves that back-pressure can *never* occur. That assertion establishes a refinement in which the missing handshake is equivalent to a permanent logical '1', so the protocol is observationally identical to a two-way handshake that trivially satisfies E2.
Combinational processes	These have no S, R, W, or M actions, so their τ_P is the empty trace. The equivalence relation therefore holds vacuously.

For the purposes of the formal analysis, non-blocking message-passing is modeled at the level of committed transfers: a successful PushNB/PopNB contributes the same committed Push_c/Pop_c event to Σ as a blocking Push/Pop, while unsuccessful polls are ε-steps.

If a design contains latency-sensitive global signals or non-blocking transfers whose timing/ordering is externally visible at the DUT boundary and must be reproduced exactly in both simulations, we take as an axiom that a purely synchronizing snooping wrapper can be applied to supply the same latency choices to the pre-HLS simulation as those observed in the post-HLS RTL (Appendix L). Conceptually, this wrapper is a witness-selection device: it does not enlarge the set of admissible pre-HLS behaviors, but restricts the pre-HLS run to one admissible execution whose Σ-events align with the observed RTL execution. Under this wrapper, the committed Σ-traces of the two simulations agree, and the equivalence rules E1–E5 apply to the wrapped runs.

Appendix L provides detailed guidance to enable this perfect alignment to be achieved in practice.

---

4. Proof Structure

The proofs proceed in three stages:
First, in Appendix I we establish per-process equivalence by showing that, under a *live environment*, every RTL process trace corresponds to a source-level trace and vice versa. Here, *live environment* does not mean assuming the entire system is deadlock-free; it refers specifically to the standard conditions of weak fairness, finite pipeline depth, and the local progress invariants (e.g., P_push(c),P_pop(c)). These are scheduling and channel-usage side-conditions, not the global liveness property that will be proved later.
Second, in Appendix J we compose these per-process results into a system-level equivalence theorem. This stage relies on channel-ordering and occupancy lemmas but does not assume system-level liveness.
Finally, Appendix K discharges the earlier "live environment" assumption by proving that system-level liveness is preserved through HLS. Specifically, if the source-level bounded-FIFO interpretation SysB (with capacities B(c) matching RTL(Sys)) is live under weak fairness, then RTL(Sys) is also live. (When B(c)=0 for all channels, SysB coincides with the rendezvous model.) This step ensures that the overall proof is non-circular: the liveness property invoked in the first stage is rigorously established only at the end.

---

5. Causal Dependency Between Processes

To prove system-level equivalence, we must distinguish between incidental timing and functionally significant ordering.

Formal Definition of Causal Dependency
To formalize the notion of functionally significant ordering and resolve ambiguity, we define the happens-before relation, denoted by ->, on the set of all observable IO actions (Σ) across all processes in the system. This relation establishes a strict partial order of events, where a -> b is read as "a happens before b".
The *happens-before* relation is the smallest relation satisfying the three conditions below:

1. Intra-Process Order: If actions a and b occur within the same process P and a precedes b in the program's execution trace, then a -> b. This directly reflects the sequential nature of the code within a single thread.

2. Inter-Process Communication: The relation is established by the direct exchange of information or synchronization between processes.

    - Message-passing (committed transfer): If a is the commit of a send on channel c in process P1 (a committed Push_c, including a successful PushNB), and b is the commit of the corresponding receive on c in process P2 (a committed Pop_c, including a successful PopNB), for the same logical message, then a → b. Unsuccessful non-blocking polls are ε-steps and do not participate in →.

    - Signal Handshake: If a is a signal write action w(sig) in P1 and b is a signal read action r(sig) in P2 that reads the value written by a as part of an explicit handshake protocol, then a -> b. A complete two-way handshake (e.g., vld/rdy) creates a causal chain, such as w(vld)@P1 -> r(vld)@P2 -> w(rdy)@P2 -> r(rdy)@P1.

- Explicit Synchronization: If a set of actions {s_1, s_2, ... s_n} across different processes participates in a single, atomic synchronization event (e.g., a SyncChannel barrier), then the completion of that event for the group happens-before any subsequent, dependent action in any of the participating processes.

3. Transitivity: The relation is transitive. If a -> b and b -> c, then a -> c.

Using this relation, we now provide a formal definition for causal dependency between synchronization events, which are the fundamental ordering anchors in the scheduling model.

Definition: Causal Dependency
A synchronization event s2 in process P2 is causally dependent on a synchronization event s1 in process P1 if and only if s1 -> s2.
If neither s1 -> s2 nor s2 -> s1 holds true, the events s1 and s2 are considered causally independent (or concurrent). Any change in the observed temporal ordering of causally independent events between the pre-HLS and post-HLS simulations is considered an incidental, functionally insignificant variation in latency. A well-formed design, under this methodology, shall not rely on a specific ordering of causally independent events for functional correctness.

To be clear, the shall not rely requirement is a design rule. To adhere to this design rule, designs must use message passing, SyncChannel operations, and signal handshakes to properly order operations across the system. Designs which violate this design rule are outside of the formal guarantees.

---

6. System-Level Theorem

Theorem (Compositional Equivalence).
Fix any test stimulus (environment inputs) and initial state. Let $\tau_{B,system}$ be the resulting observable trace of the source-level bounded-FIFO system Sys_B under that stimulus, where Sys_B denotes the same source-level processes as Sys but interpreted under E4 as abstract bounded FIFOs of capacity B(c) (the same B(c) as in RTL(Sys), see Remark 2 in Appendix J); when B(c)=0 this coincides with rendezvous system Sys under that stimulus, and let $\tau_{post,system}$ be the resulting observable trace of RTL(Sys) under the same stimulus. Assume every process P satisfies $\tau_{pre,P} \approx \tau_{post,P}$ by Appendix I, every channel c has finite capacity $B(c) \geq 0$, the progress invariants P_push(c) and P_pop(c) hold for every c, and the system satisfies weak fairness (WF). Then the aggregate traces are equivalent: $\tau_{B,system} \approx \tau_{post,system}$ under rules E1–E5 (given the R rules and B rules).
Proof sketch. (Full proof is in Appendix J – System-Level Trace Equivalence Proof)
Equivalence is defined per observable channel or signal.
By E1–E5 each process preserves:

1. ordering of synchronizing actions visible to other processes,
2. FIFO legality of every channel,
3. atomic association between signal IO and its bounding sync.
4. the *side-of-sync* predicate for all message actions (E5).

Because the composition of partial-order–preserving relationships is itself preserving, and because channels/signals are the only inter-process observables, system-level behavior is bisimilar under the relation ≈.

---

7. Practical Implication (“No Surprises” Guarantee)

If a verification environment exercises only the alphabet Σ (signals, message ports, synchronization calls) and does not test internal latency, then any testbench that passes on the pre-HLS model is *provably*

guaranteed to pass on the post-HLS RTL, provided the design obeys the scheduling rules. This justifies single-testbench methodologies.

Appendix G thus establishes that the scheduling rules create a *trace-equivalence* relation between the high-level model and the synthesized RTL: every legal compiler optimization is a morphism of the labeled partial-order structure defined by R1–R5, ensuring functional indistinguishability at all observable interfaces.

Appendix H – Possible Criticisms

This section highlights several potential challenges in the verification approach of Appendix G.

1. Designer-Managed Shared-Memory Synchronization

Appendix G requires that any memory shared between processes use explicit synchronization primitives inserted by the designer. The HLS tool does not perform static verification of those primitives. In practice, we mitigate this risk by encapsulating shared memories within parameterized library classes (for example, see examples 12_ping_pong_mem and 15_native_ram_fifo) that are pre-verified for correct memory access coordination in both the pre-HLS and post-HLS models. Typically such classes will be parameterized for aspects such as element type and memory size.

2. Latency-Sensitive Signal Alignment (“Snooping”)

See Appendix L for detailed discussion on snooping.

3. Matchlib Connections by Default Model a Skidbuffer inside In<> Ports

(Note that this overall document and specifically Appendix G are not intended to be strictly tied to Matchlib. Instead, this document is intended to be applicable to any pre-HLS model written in SystemC using signals, message-passing channels, and synchronization calls.)

Matchlib Connections supports throughput accurate modeling in the pre-HLS simulation. Currently the throughput accurate modeling mechanism relies on the Pre() and the Post() methods using a 1-place buffer to store transactions that are in flight on Connections::In<> ports. This means that by default In<> ports function like a skidbuffer. Connections::Out<> ports do not introduce any additional storage capacity into the pre-HLS simulation.

By default, Catapult adds skidbuffers on input ports into the post-HLS design, so the formal equivalence relationship described in this document still holds. In other words, the default pre-HLS and post-HLS designs both still model rendezvous semantics, since both explicitly include a structural instantiation of a skidbuffer on input ports. In effect, we define the rendezvous boundary *before* the skidbuffer.

It is possible to remove some or all the skidbuffers during Catapult HLS. Because the abstract rendezvous boundary is defined before the skidbuffer, this choice is orthogonal to the equivalence rules

(R1–R5/E1–E5) as long as skidbuffer-internal behavior is not included in Σ. However, to keep the pre-HLS simulation's *port micro-architecture* aligned with the RTL configuration, the following compile flag must then be used in this case:

```
-DFORCE_AUTO_PORT=Connections::SYN_PORT
```

This will remove all the skidbuffers from the pre-HLS model. If some of the skidbuffers are still inserted during HLS, the formal equivalence relationship will still hold provided skidbuffer capacity is accounted for properly within Sys_B.

In this case the recommended methodology is to use both approaches:

- Use the default throughput accurate mode in Matchlib for most analysis and debug, and for pre-HLS performance verification.

- To keep the pre-HLS simulation's *port micro-architecture* strictly aligned with the RTL configuration, then use -DFORCE_AUTO_PORT=Connections::SYN_PORT, and rerun final verification tests.

Common Formal Definitions for Appendices I-K

Throughout Appendices I–K, the formal comparison is between RTL(Sys) and Sys_B, i.e., the same source processes interpreted under bounded-FIFO semantics with capacities B(c) matching the RTL (E4). The rendezvous model is recovered as the special case B(c)=0.

Symbol / Rule	Definition — concise but complete
Σ	Set of observable actions for the equivalence check (committed IO events) at the chosen observable boundary (often the DUT IO boundary for functional equivalence, but optionally expanded—e.g., for Appendix K deadlock reasoning): • channel commit events Push_c(v) and Pop_c(v) on channels designated as observable, labeled with the transferred message value (or abstract message identity) v • synchronization events wait(), Sync, START_P, FINISH_P • single-cycle signal actions Write(sig, val) and Read(sig, val) on signals designated as observable, labeled with the value written/read. Internal-only channels/signals may be excluded from Σ (treated as ε-microstate) when they are not part of the chosen observable boundary. If such channels/signals are later brought into the observable boundary (e.g., by snooping for debug or analysis), then they become Σ-events and must match under ≈. Deadlock-analysis requirement (Appendix K): for Appendix K, Σ is instantiated to include every message-passing channel that can participate in deadlock reasoning (i.e., can contribute a dependency edge in the Appendix K Wait-For Graph via a potentially blocking Push_c/Pop_c), either because it is on the declared observable boundary or because it is snooped. Non-blocking message-passing (PushNB/PopNB): A non-blocking call that returns "not completed" produces no Σ-event and is modeled as an internal ε-step. When a non-blocking call succeeds (returns "completed"), that success is represented in Σ as the

Symbol / Rule	Definition — concise but complete
	corresponding committed Push_c(v) or Pop_c(v) event on that channel, labeled with the same transferred value/message v (i.e., Σ records transfers and their payloads, not failed polls).
START_P	First observable action emitted by process P after reset. Marks the moment P begins executing user code. A new START_P is emitted each time P exits reset.
FINISH_P	Last observable action of process P. If P executes an unbounded loop, FINISH_P never occurs, and the trace is treated as infinite.
ε-step	An *internal*, unobservable RTL state transition (pipeline advance, FSM micro-state, etc.).
B(c)	Compile-time *capacity* of channel *c* chosen by the HLS tool. Finite, B(c) **≥** 0. • B(c)=0 ⇒ rendezvous (capacity-zero) channel. • B(c)>0 ⇒ bounded FIFO. Point-to-point endpoint assumption (single-producer/single-consumer): For every message-passing channel c (including both buffered channels with B(c)>0 and rendezvous channels with B(c)=0), there is exactly one producer process that may execute Pushc on c, and exactly one consumer process that may execute Popc on c. Hence the complementary endpoint relevant to any blocked Pushc/Popc on c is unique. Modeling note (shared resources / arbitration): If an implementation conceptually has multiple producers and/or multiple consumers for a logical resource, that sharing must be modeled explicitly (e.g., an arbiter process plus per-client point-to-point channels), rather than as a single multi-endpoint "channel." This keeps WFG wait dependencies well-defined and unique per edge.
occ_c(t)	*Occupancy* of channel *c* after cycle *t*: number of committed Push_c minus committed Pop_c.
P_push(c)	*Finite-progress invariant (producer):* interpret "continuously enabled" as a persistent (non-withdrawable; no deassert-before-commit) ready/valid request. If the producer's Push_c request remains asserted continuously from some cycle t_o onward while the channel is full (occ_c = B(c))—with stable payload while asserted—and the complementary endpoint continuously requests the matching Pop_c (persistent request asserted; Pop_c local guard remains true), then some future cycle $t'>t_o$ commits a complementary Pop_c (i.e., the full condition is eventually discharged).
P_pop(c)	*Finite-progress invariant (consumer):* interpret "continuously enabled" as a persistent (non-withdrawable; no deassert-before-commit) ready/valid request. If the consumer's Pop_c request remains asserted continuously from some cycle t_o onward while the channel is empty (occ_c = 0)—and the complementary endpoint continuously requests the matching Push_c (persistent request asserted with stable payload; Push_c local guard remains true)—then some future cycle $t'>t_o$ commits a complementary Push_c (i.e., the empty condition is eventually discharged).
Equivalence rules (E1–E5)	*E1 Synchronization-order preservation*: For each process P, the sequence of synchronization events executed by P (wait(), SyncChannel, START_P, FINISH_P) appears in the same source order in the pre-HLS and post-HLS traces. *E2 Signal visibility*: For each process P, each signal Read in P occurs at the closest preceding synchronization event in P, and each signal Write in P occurs at the closest

Symbol / Rule	Definition — concise but complete
	succeeding synchronization event in P, in both the pre-HLS and post-HLS traces (per R2/E2) (except explicitly declared direct-input exceptions). Interpretation (logical timestamping). The equations in E2 define the logical timestamps of Read/Write Σ-events (the anchor points at which equivalence is checked). An implementation may physically sample a Read later than pred_S(r) (or physically apply a Write earlier than succ_S(w)) provided the value is stable across the anchor interval and the trace emitted for equivalence records the Σ-event at the anchor point (see the Instrumentation note in Appendix G). Direct-input pragmas (e.g., #pragma hls_direct_input and #pragma hls_direct_input_sync) are not exceptions to E2: they impose stability/timing contracts that allow late physical sampling (or controlled updates) while the logical Read/Write Σ-events used for ≈ checking remain timestamped at the E2 anchor points (see Appendix G, Direct Inputs and Instrumentation note). *E3 (Safe message issue ordering; pipelined-loop read-ahead permitted).* For any two message operations m1,m2 ∈ M issued by the same process: (i) Same-interface order is always preserved: if m1 and m2 access the same message-passing interface/channel and m1 <_src m2, then issue_post(m1) ≤ issue_post(m2). (ii) Distinct-interface no-reverse holds except for pipelined-loop read-ahead: if m1 and m2 access distinct message-passing interfaces and appear in sequence in the source, then they shall not be issued in reverse order unless they are a pipelined-loop read-ahead case as described in “Pipelined Loops” (i.e., a message-passing read from a younger overlapped iteration issued before a message-passing write from an older iteration). In that pipelined-loop read-ahead case, reverse issue order is permitted, and deadlock risks are addressed by the automatic flush discipline described in “Pipelined Loops” and Appendix K. *E4 FIFO legality*: for each channel c, the post-HLS committed (Push_c(v), Pop_c(v)) history is a legal bounded-capacity execution consistent with Sys_B for that channel (capacity B(c)), and reduces to rendezvous consistency when B(c)=0. In particular, on each channel, the committed Pop_c(v) events return exactly the FIFO-ordered sequence of values v previously committed by Push_c(v), with no drops, duplications, or reordering. *E5 Side-of-Sync guarantee*: a message action never moves across its bounding synchronization event (START_P, FINISH_P, explicit wait/Sync).

Additional Semantic Assumptions (B-rules)

The following B rules are process assumptions used within the formal proofs. These B rules are in addition to the R rules presented in Appendix G.

ID	Basic-process property (informal statement)	Why it is needed / how it is used
B1 Deterministic Trace Property	For any fixed test stimulus and initial state, the sequence of observable actions emitted by the post-HLS design is unique, including the channel identity and payload/value of each	Ensures the per-process and system-level equivalence proofs (App. I & J) can match *one* post-HLS trace to *one* pre-HLS trace without

ID	Basic-process property (informal statement)	Why it is needed / how it is used
	committed Push_c(v)/Pop_c(v) and the value of each Write(sig,val)/Read(sig,val). Internal ε-steps may differ between runs, but the externally visible Σ-trace (with labels) cannot.	branching on scheduler nondeterminism.
B2 Weak Fairness of the Scheduler (WF)	If an action's enabling predicate remains continuously true from cycle *t* onward, the scheduler must eventually select that action (within a finite, but unspecified, number of cycles). Applies to Push, Pop, and Sync operations.	Required for all progress arguments, especially the liveness lemmas in Appendix K and the channel-progress corollaries.
B3 Channel Progress Invariants	For every channel *c* with capacity B(c): • P_push(c): If a process P is stalled at a blocking $Push_t(c)$ with its local guard true and a persistent request asserted (payload stable, if applicable) while the channel is full ($occ_t(c)$ = B(c)), and the complementary endpoint process continuously requests the matching $Pop_t(c)$ (persistent request asserted; $Pop_t(c)$ local guard remains true), then the transfer on *c* must eventually complete (in particular: for B(c)>0, some $Pop_t(c)$ eventually commits, freeing space; for B(c)=0, the rendezvous completion eventually occurs). • P_pop(c): If a process P is stalled at a blocking $Pop_t(c)$ with its local guard true and a persistent request asserted while the channel is empty ($occ_t(c)$ = 0), and the complementary endpoint process continuously requests the matching $Push_t(c)$ (persistent request asserted with stable payload; $Push_t(c)$ local guard remains true), then the transfer on *c* must eventually complete (in particular: for B(c)>0, some $Push_t(c)$ eventually commits, providing data; for B(c)=0, the rendezvous completion eventually occurs).	Explicitly assumed in Appendix J to rule out permanent back-pressure loops in which both endpoints continuously request a transfer but it never completes, which are logically independent of the cycle-by-cycle R-rules.
B4 Finite Stutter Bound	Every process P has a finite constant depth D_P such that whenever P is not externally stalled (i.e., P is advancing internal micro-state toward its next observable Σ-action, or its next Σ-action is locally enabled), P can execute at most D_P consecutive ε-steps before either (i) executing a Σ-action, or (ii) reaching a stable waiting state in which P has no further ε-step available until some	This guarantees the ε-stutter closure needed to construct witness mappings in Appendix I and to bound internal micro-latency (pipeline/FSM bookkeeping) by ≤ D_P. Unbounded waiting due to back-pressure or missing peer stimulus is governed by WF/B2 and the progress obligations B3, not by B4.

ID	Basic-process property (informal statement)	Why it is needed / how it is used
	external/peer/environment condition changes the enabling predicates.	
B5 System Quiescence Closure	If, at some cycle t_o, no observable actions are enabled in any process, then within at most max_P D_P further cycles the system reaches a fixed point and executes no additional ε-steps.	Needed to finish the starvation-vs-deadlock analysis in Appendix K: ensures an all-disabled state cannot hide behind an infinite tail of unobservable activity.

Appendix I – Per Process Trace Equivalence Proof

I.1 Overview

For any single source-level process P that obeys the basic R rules and B rules, interpreted under Sys_B bounded-FIFO semantics with finite capacities B(c) ≥ 0 (matching the post-HLS RTL), every finite observable trace produced by P has a matching post-HLS RTL trace that satisfies E1–E5. Rendezvous channels are the special case B(c)=0.

I.2 Formal Preconditions

- Observable alphabet Σ is as defined in *Common Formal Definitions for Appendices I–K*: it consists of the event schemas {Push_c, Pop_c, Sync, wait, START_P, FINISH_P, Write, Read} instantiated only for channels/signals designated observable; additionally, all message-passing channels that can participate in Appendix K deadlock reasoning are designated observable (possibly via snooping) and hence included in Σ.
  Non-blocking message-passing interpretation. A successful non-blocking PushNB/PopNB contributes the same observable event as the corresponding committed Push_c/Pop_c on that channel. An unsuccessful non-blocking call (returns "false" / "not completed") contributes no Σ-event and is modeled as an ε-step.
- Silent step Any internal RTL microstate transition is written **ε**. In particular, unsuccessful non-blocking polls, arbitration bookkeeping, and pipeline advances are ε-steps.
- Finite-pipeline-depth premise (FPD) There exists a finite constant pipe_depth(P) = D_P < ∞ such that once P begins internal micro-progress toward its next observable Σ-action (or that next Σ-action is locally enabled), P executes at most D_P cycles of ε-steps before either committing a Σ-action or reaching a stable waiting state with no further ε-step available until external/peer conditions change. In particular, a process cannot perform an unbounded number of ε-only failed non-blocking polls while making no progress toward any Σ-action; designs that can spin indefinitely without reaching either a Σ-action or a stable wait state violate FPD/B4 and are outside the model.
- Weak-fairness premise (WF) If a micro-operation remains continuously enabled, the scheduler eventually issues it. This is an assumption on the execution/scheduling environment (See Appendix N), not an automatic guarantee of "clock-synchronous RTL." In practice it requires that any arbiters/back-pressure logic that can affect whether an enabled operation is selected must be fair in the sense of B2/B3.

- Finite-progress invariants (B3) For every channel c, assume producer and consumer obligations P_push(c) and P_pop(c) hold, guaranteeing that data (or space) eventually becomes available. This is an assumption on the execution/scheduling environment (e.g., fairness of arbiters/back-pressure; see Appendix N), not a consequence of the cycle-by-cycle R-rules.
- Pure-FIFO channel semantics. For any message-passing channel *c* with *B(c) > 0*: if a process has issued a persistent request to transfer on *c* (i.e., the request remains asserted and the payload is stable, if applicable), then the channel-side commit-enabling predicate is exactly the FIFO availability predicate—namely:
    - for Push_c: *occ_c < B(c)* ("not full"), and
    - for Pop_c: *occ_c > 0* ("not empty").

  No additional arbitration/grant/back-pressure gating is part of the channel semantics; any such gating must be modeled as part of the process local guard or as an explicit synchronization/wait, not inside the channel.
  Therefore, when the local guard is true and the relevant FIFO availability predicate holds continuously, the transfer is continuously enabled; by weak fairness (B2) the corresponding commit occurs after a finite (though not necessarily bounded) delay.
- No ill-formed signal IO Every signal read/write has a unique bounding synchronization operation in the source program; otherwise, the design is ill-formed. (From RULE 1 and RULE 2).

I.3 Auxiliary Lemmas

Lemma I.0 (Message-issue discipline in RTL).

The RTL satisfies E3: (i) per-interface issue order is preserved for all message operations; and (ii) for distinct interfaces, the no-reverse rule holds except for the pipelined-loop read-ahead case permitted by "Pipelined Loops."

Lemma I.1 (Bounded **ε**-chain to **Σ**-action or stable wait). Starting from any state of P, within at most D_P clock cycles P either (i) commits its next observable Σ-action, or (ii) reaches a stable waiting state with no further ε-step available until some external/peer condition changes the enabling predicates.

Proof. Direct from FPD/B4. ■

Lemma I.2 (Eventual space / data). Assume P is blocked on • Push_c with occ_c = B(c), and the complementary endpoint continuously requests the matching Pop_c (persistent request asserted; Pop_c local guard remains true), or • Pop_c with occ_c = 0, and the complementary endpoint continuously requests the matching Push_c (persistent request asserted with stable payload; Push_c local guard remains true). Then a complementary Pop_c (respectively Push_c) commits within finite time.

Proof. (By B3 / Appendix N.) In either case, P is stalled at a blocking channel call while its persistent request for that call remains asserted (payload stable, if applicable). By the additional premise, the complementary endpoint also continuously requests the matching operation with its local guard remaining true. Therefore the premises of P_push/P_pop (Appendix N) hold, and the corresponding transfer must eventually complete: for Push_c at full, some complementary Pop_c eventually commits (freeing space); for Pop_c at empty, some complementary Push_c eventually commits (providing data). ■

I.4 Inductive Construction for Finite Traces

Let

$\tau\_pre = \tau\_pre[0..n-1] \circ e$ (where $|\tau\_pre| = n + 1$)

be the next pre-HLS prefix. Assume by induction that we already have a matching post-HLS prefix $\tau\_post[0..n-1]$ satisfying E1–E5. We extend it with a finite ε-chain (written ε*) followed by an observable action e' so that

$\tau\_post \circ \varepsilon^* \circ e'$ matches τ_pre.

Non-blocking note. For a non-blocking PopNB/PushNB, each unsuccessful poll is an ε-step (unobservable), and the first successful completion is represented as the corresponding committed Pop_c/Push_c event in Σ. Therefore, non-blocking message-passing is handled by the existing Push_c / Pop_c rows of the construction table (Σ records committed transfers, not failed polls).

Kind of event *e*	Why **ε*** is finite
Sync, wait, START_P, FINISH_P, Write, Read	• Internal pipeline/microstate progress for P to reach the blocked state at this operation is bounded by ≤ D_P ε-steps (Lemma I.1). Completion of Sync (or wait) may then require peer/environment enabling and may therefore be delayed by an a priori unbounded number of cycles while P is externally stalled. However, RTL(Sys) is assumed to have no scheduler nondeterminism under a fixed stimulus/initial state (B1), so the RTL(Sys) execution under that stimulus is unique at the Σ level. Under the fixed-stimulus comparison (same external stimulus/peer behavior for Sys_B and RTL(Sys)), if the event completes in Sys_B then the corresponding peer/environment enabling must occur at some finite time under that same stimulus in RTL(Sys) as well. This peer/environment enabling is part of the compared stimulus/peer behavior; it is not implied by weak fairness (B2), nor by the channel progress invariants (B3, which apply only to message channels). Once the enabling condition has occurred so that completion of the event is continuously enabled, weak fairness (B2) guarantees that the scheduler selects it after a further finite (though not necessarily bounded) delay. Thus the matching observable event e′ occurs after a finite (though not necessarily bounded) delay.
Push_c	• issue_post(e′) occurs when P reaches and issues the Push_c operation (i.e., when Push_c is one of P's next enabled Σ-actions with its local guard true). Lemma I.0 guarantees the required source-order issue discipline for message operations (E3). • If B(c) > 0 and the transfer's commit-enabling predicate holds continuously (pure-FIFO: in particular *occ_c* < *B(c)* for Push_c), then the transfer is continuously enabled; by weak fairness (B2) the scheduler selects it after a finite (though not necessarily bounded) delay, so the commit occurs after finitely many ε-steps. • If *B(c) > 0* and occ_c = *B(c)*: Lemma I.2 frees space. • If *B(c) = 0*: rendezvous fires when both sides are enabled; Lemma I.2 guarantees eventual completion given both sides continuously request.
Pop_c	Symmetric to Push_c (pure-FIFO: for Pop_c with B(c) > 0, the availability predicate is *occ_c > 0*).

Each case ensures ε* terminates, so the extension preserves E1–E5; in particular, the issue-order clause of E3 is satisfied via Lemma I.0. ■

I.5 Extension to Infinite Traces

Fix a process P and a fixed external stimulus/initial state. Let τ_B,P be the (countably infinite) observable trace of P in the source-level bounded-FIFO interpretation Sys_B.

We construct an infinite post-HLS trace τ_post,P by an explicit inductive limit of the finite-prefix construction in I.4.

Let τ_post,P[0..0) be the empty prefix. For each n ≥ 0, assume we have constructed a finite post-HLS prefix τ_post,P[0..n) such that its Σ-projection matches the first n observable events of τ_B,P and the correspondence satisfies E1–E5. Let e_n be the (n+1)-st Σ-event of τ_B,P. Apply the I.4 construction step

to extend τ_post,P[0..n) by a finite ε* segment followed by a matching observable event e′_n, obtaining τ_post,P[0..n+1) while preserving E1–E5.
Because each extension step adds a finite segment, the increasing chain of prefixes defines a (countably infinite) post-HLS trace τ_post,P whose every finite prefix matches the corresponding prefix of τ_B,P. Therefore, τ_B,P ≈ τ_post,P (for countably infinite traces as well). ■

Appendix J – System-Level Trace Equivalence Proof

Theorem J.1 (Compositional Equivalence)
Fix any test stimulus (environment inputs) and initial state. Let τ_B,system be an observable trace of the source-level bounded-FIFO system Sys_B under that stimulus, and let τ_post,system be an observable trace of RTL(Sys) under the same stimulus. (If B1 holds, each is unique for the given stimulus/initial state.) Assume every process P satisfies τ_B,P ≈ τ_post,P by Appendix I, where τ_B,P is the projection of the Sys_B system trace τ_B,system onto P, every channel c has finite capacity B(c) ≥ 0, the progress invariants P_push(c) and P_pop(c) hold for every c, and the system satisfies weak fairness (WF). Assume also B1 (Deterministic Trace Property) when uniqueness of the trace is relied upon. Then the aggregate traces are equivalent: τ_B,system ≈ τ_post,system under rules E1–E5 (given the R rules and B rules).
Notation: Let <_src denote the textual order of operations within a single process in the source code.
Proof
We first establish key invariants, then prove each equivalence property.
Lemma J.1 (Channel Occupancy Invariant)
For every channel c and at every clock cycle t in the post-HLS execution, the occupancy occ_post(c,t) satisfies 0 ≤ occ_post(c,t) ≤ B(c).
Proof of Lemma J.1:
We argue by cases on B(c).
If B(c) > 0 (buffered FIFO): RTL never de-queues from an empty FIFO and never en-queues into a full FIFO. A Push_c can only commit when occ(c) < B(c) and a Pop_c can only commit when occ(c) > 0, so the occupancy stays within 0..B(c) by induction.
If B(c) = 0 (rendezvous): a transfer can commit only when the complementary endpoint is enabled in the same cycle (Push_c and Pop_c commit together), so the cycle-aligned occupancy is always 0 and thus satisfies 0 ≤ occ(c,t) ≤ B(c)=0 at every cycle.
Lemma J.2 (Per-Channel Push/Pop Precedence)
Fix a channel c. Let Push_c[k] denote the k-th committed Push on c in the post-HLS execution, and Pop_c[k] denote the k-th committed Pop on c (k ≥ 1). Under the single-op-per-cycle endpoint constraint, at most one Push_c and at most one Pop_c can commit per cycle, so these "k-th" events are unambiguous. Then: clk_post(Push_c[k]) ≤ clk_post(Pop_c[k]).
Proof of Lemma J.2:

- For B(c)=0 (rendezvous), Push_c[k] and Pop_c[k] commit simultaneously, so equality holds.
- For B(c)>0, a Pop can only commit when the FIFO is non-empty. After i committed Pushes and j committed Pops, occupancy is i–j. For Pop_c[k] to commit, immediately before it commits we must have i–j > 0, hence i ≥ j+1 = k. Therefore the k-th Push has already committed by that time, i.e., clk_post(Push_c[k]) ≤ clk_post(Pop_c[k]). □

We now prove each equivalence property:
E1 (Synchronization-order preservation):

Fix any process P. By Appendix I, $\tau_{B,P} \approx \tau_{post,P}$, so the synchronization events of P occur in the same source order in both traces. Since this holds for every P, E1 holds for the system traces $\tau_{B,system}$ and $\tau_{post,system}$.

E2 (Signal-visibility preservation):

Fix any process P. By Appendix I (and rule R2 as used there), every signal Read in P is anchored to P's closest preceding synchronization event, and every signal Write in P is anchored to P's closest succeeding synchronization event, in both $\tau_{B,P}$ and $\tau_{post,P}$. Since this holds for every P, E2 holds for $\tau_{B,system}$ and $\tau_{post,system}$.

E3 (Safe message issue ordering):

Fix any process P. We must show that P's post-HLS execution satisfies E3 as stated in Appendix G: (i) for same-interface pairs m1,m2 with $m1 <_{src} m2$, we have $issue_{post}(m1) \leq issue_{post}(m2)$; and (ii) for distinct interfaces that appear in sequence in the source, the operations are not issued in reverse order except in the permitted pipelined-loop read-ahead case described in "Pipelined Loops" (with deadlock risks addressed by automatic flush / Appendix K).

This is exactly the per-process property established in Appendix I (Lemma I.0). Since it holds for every P, E3 holds for the system traces $\tau_{B,system}$ and $\tau_{post,system}$.

E4 (Per-channel FIFO semantics):

For each channel c, we must show:

1. The sequence of Push_c and Pop_c operations in τ_{post} forms a legal FIFO schedule
2. No messages are dropped or duplicated
3. FIFO order is preserved in the Σ-trace sense: if a committed transfer m1 precedes m2 in the per-channel (Push_c/Pop_c) history required by Sys_B/E4, then the corresponding committed transfers appear in the same order in τ_{post} on that channel.

From Appendix I, each process preserves the order of its operations on each channel. Lemma J.1 establishes that $0 \leq occ_{post}(c,t) \leq B(c)$ at all times, and Lemma J.2 establishes that, for each channel c, the k-th Pop cannot commit before the k-th Push. Together these imply:

- Pops never underflow and Pushes never overflow the bounded FIFO (legality).
- Each committed Pop consumes exactly one previously committed Push, in FIFO order (no drops/duplication; FIFO order preserved).
- Capacity constraints are respected at every clock cycle.

Therefore, the post-HLS (Push_c, Pop_c) history on each channel is a legal bounded-FIFO execution consistent with the source-level FIFO semantics required by E4.

E5 (Messages cannot cross syncs):

For any message operation m and synchronization call s in the same process P:

- If $clk_{pre}(m) \leq clk_{pre}(s)$, then $clk_{post}(m) \leq clk_{post}(s)$
- If $issue_{pre}(m) >= clk_{pre}(s)$, then $issue_{post}(m) >= clk_{post}(s)$

This property is guaranteed per-process by Appendix I and requires no inter-process reasoning, so it lifts directly to the system level.

Conclusion:

All five equivalence properties hold at the system level. The composition is valid because:

- Intra-process properties are preserved by Appendix I
- Inter-process communication respects capacity bounds (Lemma J.1) and ordering (Lemma J.2)
- The progress invariants and weak fairness ensure the matching construction can always advance (i.e., executions do not diverge via permanent stalling on enabled actions).

Therefore, $\tau_{B,system} \approx \tau_{post,system}$. □

Remark 1. When all B(c)=0, Sys_B coincides with the rendezvous interpretation of Sys, so the theorem specializes to the rendezvous case.

Remark 2. The Matchlib library has a capacity back-annotation feature that enables the pre-HLS model to automatically incorporate channel capacity information from the RTL design.
Remark 3 (Practical rendezvous screening under determinism). When B1 holds and the design's control flow does not branch on empty/full observations of non-blocking interfaces (i.e., it depends only on the ordered history of observable Push/Pop/synchronization actions, not on "probe" outcomes), the rendezvous specialization B(c)=0 is often an effective *practical* screen for design-level deadlocks: it exercises the most constrained communication discipline and can expose true cyclic data-dependency deadlocks early. However, bounded buffering can still introduce capacity artifacts ("artificial" deadlocks) when FIFO depths are underestimated; increasing buffer capacity (or applying dynamic buffer-growth strategies) is a standard way to separate such capacity artifacts from real dependency deadlocks. Accordingly, the formal results of Appendices J–K deliberately target Sys_B with the *actual* back-annotated capacities B(c), rather than relying on rendezvous alone.
Remark 4 (When Sys may be used instead of Sys_B for safety-only checks).
If verification is concerned only with safety properties over the chosen DUT-boundary alphabet Σ (and not with deadlock/liveness), Sys_B remains the default reference model because Σ includes committed channel-transfer events, and bounded buffering (B(c) > 0) generally changes the set/timing of those committed Push_c/Pop_c events relative to the rendezvous (B(c)=0) case.
Important (soundness): When any channel that can influence Σ-observable behavior has B(c) > 0, the rendezvous model Sys is typically an under-approximation of Sys_B / RTL(Sys) (it admits *fewer* behaviors). Therefore, using Sys in place of Sys_B is generally suitable only as a debug/screening check: a failure can be useful diagnostically, but a pass does not by itself prove Σ-safety of the buffered implementation.
Sys may be used as a proof-equivalent substitute for Sys_B only when Sys and Sys_B are Σ-equivalent for the chosen Σ (i.e., their Σ-projected trace sets coincide under the intended stimulus). A sufficient condition is that every Σ-visible channel has effective capacity zero at that boundary (so Sys_B coincides with Sys *and* buffering elsewhere cannot enable/disable/reorder Σ-events). In all other cases—i.e., if any Σ-visible channel has B(c) > 0, or if buffered internal channels can affect when Σ-events occur—use Sys_B with capacities matching RTL(Sys) (Remark 2).
Formal soundness condition. Let Traces_Σ(M) denote the set of Σ-projected traces of model M under the intended fixed stimulus. Sys may replace Sys_B for proving a universal Σ-safety property ϕ only if Traces_Σ(Sys) = Traces_Σ(Sys_B); under that condition, Sys ⊨ ϕ iff Sys_B ⊨ ϕ (and otherwise Sys is only a diagnostic/screening check as stated above).

Corollary J.1 (Execution-Level / Trace-Set Form of Theorem J.1)
Purpose This corollary makes explicit the quantifiers implicit in Theorem J.1: Appendix J is intended to relate sets of executions (under a fixed stimulus), not merely to relate a single pre-chosen pre-HLS trace to a single pre-chosen post-HLS trace.
Statement Fix an initial state and a fixed external stimulus/environment behavior (e.g., the same testbench-driven inputs) for both Sys_B and RTL(Sys), where Sys_B denotes the same source-level processes as Sys, but interpreted under the channel semantics of E4 as abstract bounded FIFOs of capacity B(c) (the same B(c) as in RTL(Sys), see Remark 2 above). (When B(c)=0 this coincides with rendezvous.)
Clarification (reactive environments). If the "stimulus" is produced by a reactive testbench/environment, interpret "fixed stimulus" as fixing the environment's behavior as a Σ-causal function of the observed Σ-history (equivalently: include the environment as part of the closed system being executed, with its own fixed initial state and fixed nondeterministic choices). Under this interpretation, whenever two runs have matched Σ-prefixes, they are subject to the same subsequent environment behavior.

Let Exec_post denote the set of finite execution prefixes of RTL(Sys) that are reachable under this stimulus and that are prefixes of at least one (infinite) execution under the same stimulus that satisfies the Appendix J fairness/progress premises; and let Exec_B denote the corresponding set of finite execution prefixes of Sys_B (defined analogously).
Under the assumptions of Theorem J.1 (per-process equivalence from Appendix I, finite capacities B(c), channel progress invariants P_push / P_pop (B3), and weak fairness (B2)), plus B1/B4/B5 when ε-normalization is needed, the following prefix-matching property holds:

- (Post → B existence) For every τ_post ∈ Exec_post, there exists τ_B ∈ Exec_B such that τ_B,system ≈ τ_post,system under E1–E5.
- (B → Post existence) Symmetrically, for every τ_B ∈ Exec_B, there exists τ_post ∈ Exec_post such that τ_B,system ≈ τ_post,system.

Moreover, when B1 holds (deterministic **Σ**-projected trace under fixed stimulus), the matching **Σ**-label sequence is unique (up to insertion/removal of finite ε-steps permitted by B4/B5). The corresponding execution prefix witness τ_B need not be unique as a stateful prefix, since Sys_B may admit multiple ε-different realizations with the same Σ-projection.
Proof (sketch) Theorem J.1 establishes that the system-level E1–E5 invariants are preserved when composing processes that individually satisfy Appendix I and when channels satisfy the stated progress/fairness assumptions. Using those invariants, construct a witness prefix by induction on the length of the chosen prefix:

1. Given a reachable *τ_post*, repeatedly extend a candidate *τ_B* so that each next observable event in *τ_post* is matched by the corresponding observable event in *τ_B*, possibly preceded by a finite ε* chain to account for micro-steps/stuttering.
2. Finiteness of each required ε* extension follows from bounded stutter (B4) plus the progress/fairness premises that rule out permanent divergence via endlessly enabled-but-never-taken steps.
3. Each inductive extension preserves E1–E5 by the same reasoning used in Appendix I's finite-prefix construction, now lifted to the system via Theorem J.1's channel and composition invariants.

This yields the required existence of a matching prefix for an arbitrary reachable prefix of either model, i.e., a trace-set (execution-level) correspondence rather than a "picked-trace" correspondence. □

Corollary J.2 (State Correspondence at the End of a Matched Observable Prefix)
Purpose This corollary serves as the bridge between trace equivalence and state correspondence needed in Appendix K. The mapping target is the source-level bounded-FIFO semantics of the design (capacity B(c)), not an unrelated rendezvous (B=0) execution state.
Statement
Assume the hypotheses of Corollary J.1 (equivalently: the system-level assumptions of Theorem J.1 for Sys_B vs RTL(Sys) under the fixed stimulus), and additionally assume B1 (deterministic observable trace), B4 (finite stutter bound), and B5 (quiescence closure). Let τ_post be any τ_post ∈ Exec_post (as defined in Corollary J.1).
Define its **ε**-normalization τ̄_post as τ_post extended by a (possibly empty) finite suffix ε* to a terminal state σ̄_post that is ε-quiescent, meaning: no further ε-step is enabled from σ̄_post (so any further progress, once enabled, must proceed via an observable Σ-action rather than additional internal ε-steps). Take ε* to be a maximal finite ε-extension of τ_post; such a maximal finite extension exists under B4 (finite stutter bound), with B5 (quiescence closure) ensuring we can treat the resulting ε-quiescent representative as the canonical endpoint for the observable prefix.
(In clauses (1)–(2) directly below, interpret sigma_post as σ̄_post, i.e., the ε-normalized terminal state. When referring below to "source-level variables," the "next observable frontier," and the "logical FIFO

state" in sigma_post, interpret those notions via the standard source-level projection/abstraction from RTL(Sys) microstate to the corresponding source-level state as used in Appendix I; micro-architectural registers and bookkeeping are ignored by this projection.)
Let Sys_B denote the same source-level processes as Sys, but interpreted under the channel semantics of E4 as abstract bounded FIFOs of capacity B(c) (the same B(c) as in RTL(Sys), see Remark 2 above). (When B(c)=0 this coincides with rendezvous.) Then there exists a finite execution prefix τ_B of Sys_B ending in some reachable state sigma_B such that:
(1) The observable prefixes match: τ_B,system ≈ τ_post,system (equivalence under E1–E5).
(2) The terminal states correspond at the source level: sigma_B ≡ sigma_post, where "≡" means:
(Note: "≡" is intentionally a frontier/enable/value correspondence (clauses (a)(b)(c)), not full micro-state equality; internal pipeline/read-ahead microstate may differ between sigma_B and sigma_post provided such differences are ε-steps that are WFG-inert as assumed in Appendix K.)
(a) For every process P, the next observable source-level frontier in program order is the same in sigma_B and sigma_post. Here the "frontier" means the set of minimal (w.r.t. P's augmented source partial order) observable items that may occur next. Concretely, this means either:

- a (possibly multi-element) set of pending message actions (Push_c and/or Pop_c) on distinct interfaces that are currently minimal candidates and may be issued and (if channel-enabled) committed in any order or together in one cycle, or
- an explicit synchronization call s, together with the same set of signal Read/Write actions that are logically anchored at s per E2.
- This frontier equality does not require the pre-HLS and post-HLS models to commit identical subsets of that message set in the same cycle; it only identifies the set of currently-minimal candidates.

(b) For every process P, and for every item x in P's next observable frontier:
(i) The source-level variables that can affect whether x is enabled have the same values in sigma_B and sigma_post.
(ii) If x produces/observes a value—i.e., x is a Push_c, or x is a signal Read/Write action (or set of such actions) anchored at the next synchronization call—then the source-level variables that determine that produced/observed value have the same values in sigma_B and sigma_post.
(iii) If x is a Pop_c, then the value returned by that Pop_c is determined by the channel's logical FIFO contents after the matched observable prefix; by E4 and the matched Push/Pop history, that logical head element is the same for sigma_B and sigma_post.
(c) For every channel c, the abstract FIFO state in sigma_B (empty/full predicate, and the logical head element when non-empty) agrees with the logical FIFO state induced by the matched Push_c/Pop_c history of (1). Physical micro-architectural realization—pipeline registers, arbitration bookkeeping, and the implementation of buffering—is abstracted away by "≡", but the logical occupancy/ordering facts induced by the matched trace are not. In particular, internal read-ahead/prefetch that merely copies the current head element into internal registers without committing Pop_c is treated as ε and does not change this abstract FIFO state; only a committed Pop_c (a Σ-event) advances the logical head/occupancy.
Proof
Step 0 (By definition, work with **ε**-normalized terminal states) By the ε-normalization defined in the Statement, w.l.o.g. assume τ_post ends in an ε-quiescent state (no ε-step is enabled); we write this terminal state as sigma_post. (If not, replace τ_post by its maximal finite ε-extension $\bar{\tau}$_post = τ_post ∘ ε*, which preserves the observable prefix and is finite by B4, with the endpoint treated as the canonical ε-quiescent representative per B5.)
Step 1 (Get a matching source-level observable prefix) Fix the external test stimulus that produced the given post-HLS prefix τ_post. By the system-level prefix-matching property (Corollary J.1) applied to

Sys_B and RTL(Sys), there exists a finite execution prefix τ_B of Sys_B under that same stimulus such that τ_B,system ≈ τ_post,system under E1–E5. Let sigma_B be the terminal state of this witness prefix τ_B.
Step 2 (Align per-process control points) Because τ_B,system ≈ τ_post,system and E1/E2/E3/E4/E5 preserve per-process same-interface order, no-reverse constraints, side-of-sync constraints, and signal anchoring at synchronization points, each process P has executed the same per-endpoint observable history in both prefixes (up to commutation/regrouping of independent distinct-interface message actions). Therefore, at the end of the prefixes, P has the same next observable frontier in both sigma_B and sigma_post (clause (2a)), including the same logically anchored signal Read/Write actions at the next synchronization call when applicable.
Step 3 (Align the relevant source-level state) Matched prefixes preserve the source-level state needed for next-action enablement and payloads exactly as in Appendix I, giving clause (2b). Clause (2c) holds because, under E4, the abstract FIFO empty/full status and logical head element are uniquely determined by the matched Push/Pop history of (1), and thus coincide in sigma_B and sigma_post.
Combining Steps 1–3 gives a terminal source-level state sigma_B with sigma_B ≡ sigma_post. □

J.3 Causal Dependency ("Happens-Before") and What System-Level Equivalence Guarantees (Informative)

The system-level result of Appendix J establishes equivalence of the *aggregate* observable behavior, i.e. τ_B,system≈τ_post,system over the alphabet Σ of channel operations, synchronization events, and signal Read/Write actions.
This equivalence is intentionally *observational*: it constrains what an external environment can distinguish at Σ, not internal RTL micro-timing.
As a consequence, Appendix J should be read as preserving functionally significant ordering, not incidental latency. Functionally significant ordering is exactly the ordering induced by the happens-before relation (→) defined in the "Causal Dependency Between Processes" section: a designer must express any required cross-process ordering using message-passing edges, explicit synchronization (e.g., barriers), or explicit signal handshakes; designs "shall not rely" on the relative order of causally independent events.
Accordingly, the system-level theorem implies the following *causality preservation* principle:

- If two synchronization anchors s1 and s2 are causally related (s1→s2), then the post-HLS execution preserves their order. This is because each elementary happens-before link is preserved: intra-process order is preserved by the per-process result; message-passing links are preserved by Lemma J.2 (clk_post(Pushc)≤clk_post(Popc)); and explicit synchronization/handshake links propagate only at clock edges under the same signal and synchronization semantics. By transitivity, the entire causal chain preserves order.
- If s1 and s2 are causally independent (neither s1→s2 nor s2→s1), then their relative order is *not* constrained by the methodology, and differences are treated as incidental latency variation; relying on such ordering is outside the formal guarantees.

This perspective is what makes the "single testbench / no surprises" implication precise: any testbench that observes only Σ and encodes its expectations through causal dependencies (channels, barriers, or explicit handshakes) cannot distinguish Sys_B (the pre-HLS model interpreted with bounded-FIFO capacities B(c) matching RTL(Sys)) from the post-HLS RTL. (The rendezvous specialization Sys with B(c)=0 is covered only under the explicit conditions of Remark 4.)

Appendix K – Liveness Preservation for Buffered Implementations

K.1 Scope, Notation, and Definition of Internal Message-Passing Deadlock

We work with a fixed design:

- System Sys_B: The collection of pre-HLS processes obeying the R-rules and B-rules, interpreted under the source-level channel semantics of E4 as abstract bounded FIFOs. Each channel c has capacity B(c) ≥ 0 (the same B(c) as in the RTL implementation, see Remark 2 in Appendix J).
- Post-HLS implementation RTL(Sys): The hardware implementation of the same processes in which each channel c is realized with finite capacity B(c) ≥ 0. In this appendix, we compare Sys_B (source-level bounded-FIFO semantics) to RTL(Sys) (micro-architectural realization). The proof does not require mapping buffered RTL states to a distinct rendezvous (B=0) state.

A global state sigma of either system consists of:

1. For each process P: a control location (program point) and local state.
2. For each channel c: its current occupancy occ(c) and contents (for buffered channels).
3. Any additional architectural state (pipeline registers, arbitration state, etc.).

We adopt the usual Wait-For Graph (WFG) abstraction, restricted to internal message-passing channels. Internal means: the producer and consumer of channel *c* are both processes of *Sys_B* / *RTL(Sys)* (i.e., both endpoints are in the modeled system).

Channels whose complementary endpoint is the external environment/testbench (DUT boundary) are excluded from the WFG and from the deadlock definition in Appendix K.

- Vertices: Processes.
- Edges: There is a directed edge P→Q via channel c if, in state σ, op is a member of P's current potentially-blocking frontier Front_P(σ), P is blocked on message passing, and Q is the complementary endpoint whose action on c is required to unblock op (i.e., Popc is required to unblock a blocked Pushc, and Pushc is required to unblock a blocked Popc). Here Front_P(σ) is the set of minimal (w.r.t. P's program-order partial order / augmented source order) blocking channel operations op∈{Pushc,Popc} whose local guards are true; Front_P(σ) may contain multiple operations on distinct interfaces (reflecting the R/E freedom to issue/commit multiple Push/Pop in one cycle). P is "blocked on message passing" iff Front_P(σ) is non-empty and every op′∈Front_P(σ) is channel-disabled (its channel-side enabling condition is false). Thus WFG edges arise only from states where no enabled frontier operation exists; and when Front_P(σ) has multiple members, P may have multiple outgoing WFG edges (one per blocked frontier op). (No deassert-before-commit assumption.) Blocking Push_c/Pop_c requests are non-withdrawable: once the request corresponding to a frontier operation is asserted, it is not deasserted before that operation commits (and Push_c payload remains stable while asserted). This rules out "try-and-withdraw" behavior for blocking transfers within the WFG abstraction. This definition applies uniformly to both buffered FIFO channels (B(c)>0, enable depends on empty/full occupancy) and rendezvous channels (B(c)=0, enable requires the complementary endpoint to be enabled in the same cycle) as defined below in K.1. Thus, a single WFG may contain edges via both buffered and rendezvous channels ("mixed WFG").
  By Assumption A6 (point-to-point channels), the complementary endpoint Q for any blocked Pushc/Popc on c is unique.
  Shared-resource note: If the RTL contains sharing that would otherwise make the complementary endpoint non-unique (e.g., multi-producer or multi-consumer access to a logical resource), that sharing is modeled as an explicit arbiter process connected to each client by point-to-point channels, so WFG edges remain well-defined.
  All WFG reasoning is over **ε**-quiescent (**ε**-normalized) global states: internal

pipeline/arbitration micro-steps are treated as **ε** and are not represented as separate WFG blocking points.

(WFG-inert **ε** premise.) We assume these ε-steps are observationally silent with respect to the WFG abstraction: for any $\sigma \xrightarrow{\varepsilon^*} \sigma'$, they do not change (i) the potentially-blocking frontier Front_P(σ) for any process P (i.e., which guarded blocking Push/Pop operations are minimal and pending), nor (ii) the truth of any local guards relevant to those frontier operations, nor (iii) the channel-side enabling status (as defined in K.1) of any op ∈ Front_P(σ). Equivalently, ε-steps do not change the channel state relevant to K.1 enabling (e.g., occ(c) for B(c)>0 buffered channels), and they do not create/remove rendezvous enablement for a frontier transfer except via Σ-visible committed Push_c/Pop_c events.

In particular (pipelined loops / overlapped iterations): when HLS introduces overlap that may initiate later-iteration message reads "early," we assume the automatic flush discipline (e.g., flush-style control such as hls_stall_mode flush) guarantees WFG-inertness. Concretely, this discipline is drain-only: if a message-passing read (blocking Pop) for the current oldest pending work is not available, the process blocks at that Pop; it does not initiate any new message-passing Pops for younger overlapped iterations while blocked, and it does not withdraw any already-asserted blocking Push/Pop request (no "try-and-withdraw" behavior). The implementation may continue to advance and complete already-started older work and may commit any resulting output Pushes until the pipeline is drained. Under this discipline, flush does not introduce a later-iteration blocking Push/Pop into Front_P(σ), so transient internal pipeline activity remains ε and does not contribute wait-for edges. Any "read-ahead" performed by overlapped younger iterations in pipelined loops is treated as internal speculation: it may prefetch/peek into internal registers, but it does not decrement occ(c) (i.e., it is not a committed Pop_c) until that Pop_c is in the process's observable frontier; otherwise, the consumption is a Σ-visible committed Pop_c event and is handled at the Sys_B level rather than as an ε-step.

If a design intentionally uses internal micro-timing to change such control decisions (e.g., a sequence of "internal" steps changes the frontier Front_P(σ) of minimal guarded blocking ops, or changes guard truth for any frontier op), then that behavior must be treated as Σ-observable (e.g., via explicit modeling/snooping) and is outside the scope of Appendix K's WFG-based deadlock preservation argument.

Non-blocking polling attempts and other purely internal actions do not contribute edges to the WFG; they are modeled as internal **ε**-steps. When a non-blocking call succeeds, that success is already represented at the Σ level as the corresponding committed Push_c/Pop_c event, but it does not itself add a wait-for edge because it is not a blocking operation.

SyncChannels and barrier well-formedness.

SyncChannel (barrier) operations are treated as pure synchronization events and are omitted from the Wait-For Graph, which tracks only blocking Push/Pop dependencies. We therefore interpret "deadlock" in this appendix as internal message-passing deadlock (i.e., a deadlocked set in which all processes are blocked on some internal Push/Pop dependency captured by the WFG). Any global stall at a barrier caused by mismatched or conditional participation (e.g., a process can permanently bypass the barrier or reach it a different number of times) is a specification-level error already present in the pre-HLS model; such stalls are not created by the HLS transformation and are excluded by an explicit barrier well-formedness assumption (A8 below), not by the internal message-passing deadlock premise. Under this assumption, omitting SyncChannels from the WFG is sound: a post-HLS deadlock implies the existence of a Push/Pop wait-cycle as characterized below.

We say that a process P is blocked on message passing in state sigma if:

- Let Front_P(sigma) be P's potentially-blocking frontier: the set of minimal (w.r.t. P's program-order partial order / augmented source order) blocking channel operations op∈{Push_c,Pop_c} whose local guards are true.
- Front_P(sigma) is non-empty, and for every op∈Front_P(sigma), that operation cannot make progress because its channel-side enabling condition is false.
- (Equivalently: P is not blocked if it has no pending guarded blocking Push/Pop, or if at least one operation in its frontier is channel-enabled; since distinct-interface operations need not be grouped, P can make progress by committing any enabled frontier operation.)

(Pure-FIFO channel-side enabling condition.)
For B(c) > 0 FIFO channels:
• Push_c is channel-enabled iff occ(c) < B(c) (space available).
• Pop_c is channel-enabled iff occ(c) > 0 (data available).
For B(c) = 0 rendezvous channels:
• Push_c / Pop_c is channel-enabled iff the complementary endpoint is also enabled in the same cycle (rendezvous completion).

An internal message-passing deadlock is a reachable state sigma in which there exists a non-empty set of processes D such that:

- Every process P in D is blocked on message passing.
- The vertices in D, together with the channels they access, form a strongly connected component in the WFG that has no outgoing edges (a closed cycle): processes in D can only wait on each other.

Intuitively, D is a set of processes that are waiting only on each other and can never be unblocked by activity elsewhere in the modeled system.
Our notion of liveness in this appendix is: Liveness = absence of internal message-passing deadlock as defined above. (Starvation of a single process in an otherwise live system is ruled out separately by weak fairness.)

K.2 Assumptions and Imported Results
K.2.1 Standing Assumptions We assume throughout Appendix K:
A1. R-rules and B-rules. The source-level model Sys_B and the post-HLS implementation RTL(Sys) satisfy the process- and channel-level semantic rules defined earlier (R-rules and B-rules).
A2. Finite Pipeline Depth (FPD). There is a global bound on the number of purely internal steps (ε-steps) that can occur between consecutive observable actions.
A3. Weak Fairness (WF) (B2). If an action remains continuously enabled (its guard remains true), the scheduler eventually selects it.
A4. Channel Progress (B3; Appendix N). For each channel c with capacity B(c), assume the progress invariants of Appendix N hold. This is an obligation on the scheduler/environment (e.g., fairness of arbiters/back-pressure) and is not implied by the local R-rules alone:
• P_push(c): If a process P is stalled at a blocking Push_c with a persistent (non-withdrawable; no deassert-before-commit) request asserted, and the complementary endpoint process Q continuously has the matching Pop_c pending as a frontier operation (i.e., Pop_c ∈ Front_Q(σ) continuously, with its local guard remaining true), then the transfer on c must eventually complete (in particular: for B(c)>0, some complementary Pop_c eventually commits, freeing space; for B(c)=0, the rendezvous completion eventually occurs).
• P_pop(c): If a process P is stalled at a blocking Pop_c with a persistent (non-withdrawable; no deassert-before-commit) request asserted, and the complementary endpoint process Q continuously has the matching Push_c pending as a frontier operation (i.e., Push_c ∈ Front_Q(σ) continuously, with its local guard remaining true), then the transfer on c must eventually complete (in particular: for B(c)>0,

some complementary Push_c eventually commits, providing data; for B(c)=0, the rendezvous completion eventually occurs).
A5. Source-Level Liveness Assumption. The source-level bounded-FIFO system Sys_B (with capacities B(c) as defined in K.1) is deadlock-free under assumptions A1–A4.
A6. Point-to-point channels (single-producer/single-consumer). For each message-passing channel c (including buffered channels with B(c)>0 and rendezvous channels with B(c)=0), exactly one process performs all Pushc operations on c (the producer) and exactly one process performs all Popc operations on c (the consumer). Hence the complementary endpoint for any blocked Pushc/Popc is unique, and WFG edges are well-defined even for mixed WFGs that include both buffered and rendezvous channels.
If a design has a shared resource that would violate this uniqueness, it must be modeled via an explicit arbiter process plus point-to-point channels (as noted in K.1).
A7. Deterministic **Σ** behavior (B1) and **ε**-normalization (B4/B5).
Throughout Appendix K we assume B1 holds for both Sys_B and RTL(Sys) under the fixed stimulus/initial state (i.e., the **Σ**-projected behavior is deterministic, hence the matched Σ-prefix used in the K.5 contradiction argument is well-defined/unique up to insertion/removal of finite ε-steps).
We also rely on B4 and B5 (Appendix N) to justify **ε**-normalization / **ε**-quiescent endpoints, as required by Corollary J.2 (state correspondence).
A8. Barrier well-formedness (SyncChannels). For each SyncChannel instance, the set of designated participant processes reaches the barrier the same number of times under the fixed stimulus/initial state; equivalently, no participant can permanently bypass a barrier call while another participant is waiting at that barrier. (Barrier stalls are therefore outside the behaviors considered in Appendix K's internal message-passing deadlock analysis.)

K.3 Lemma K.1 — Characterization of Internal Message-Passing Deadlock (Buffered and Rendezvous Cases)
Statement: Let sigma_post be a reachable ε-quiescent global state of the post-HLS system RTL(Sys) (equivalently, the ε-normalization of some reachable state, which exists as a finite extension by B4/B5). Suppose there is a non-empty set of processes D that is internally message-passing deadlocked (as defined in K.1). Then:
Every process P in D is blocked on a blocking channel operation (Push or Pop), not on an internal step.
Buffered-channel case (B(c) > 0):
• If P is blocked on Push_c and B(c) > 0, then occ(c) = B(c) (channel is full).
• If P is blocked on Pop_c and B(c) > 0, then occ(c) = 0 (channel is empty).
Rendezvous case (B(c) = 0):
• If P is blocked on Push_c and B(c) = 0, then the complementary endpoint is not simultaneously enabled for Pop_c in sigma_post (i.e., rendezvous enabling for this transfer is false).
• If P is blocked on Pop_c and B(c) = 0, then the complementary endpoint is not simultaneously enabled for Push_c in sigma_post.
The processes in D form a closed strongly connected component in the WFG.
Proof:
Internal Steps: If a process were blocked on an internal step with a true guard, Weak Fairness and Finite Pipeline Depth guarantee it would proceed. Thus, deadlocked processes must be blocked on channel operations.
Blocked Push: By the definition of "blocked on message passing" in K.1, if P is blocked due to a frontier Push_c, then Push_c's local guard is true (so Push_c ∈ Front_P(sigma_post)) and the channel-side enabling condition for Push_c is false.

• If B(c) > 0, the channel-side enabling condition for Push_c is space availability, i.e., occ(c) < B(c). Hence, if P is blocked on Push_c in sigma_post, necessarily occ(c)=B(c) (channel is full).
• If B(c) = 0 (rendezvous), the channel-side enabling condition is "the complementary Pop_c endpoint is enabled in the same cycle" (K.1). Since P is blocked, this rendezvous enabling condition is false; equivalently, the complementary endpoint is not simultaneously enabled for Pop_c in sigma_post.
Blocked Pop: Symmetric. By the definition of "blocked on message passing," if P is blocked due to a frontier Pop_c, then Pop_c's local guard is true (so Pop_c ∈ Front_P(sigma_post)) and the channel-side enabling condition for Pop_c is false.
• If B(c) > 0, the channel-side enabling condition for Pop_c is data availability, i.e., occ(c) > 0. Hence occ(c)=0 (channel is empty).
• If B(c) = 0 (rendezvous), the enabling condition is "the complementary Push_c endpoint is enabled in the same cycle." Since P is blocked, the complementary endpoint is not simultaneously enabled for Push_c in sigma_post.
Closed Cycle: By definition of internal message-passing deadlock, processes in D cannot wait on processes outside D, or else an external action could unblock them.
K.4 Lemma K.2 — Dependency Refinement
We now relate the blocking dependencies in the RTL buffered system to those in the source-level bounded-FIFO semantics Sys_B.
Statement: For any pair of corresponding states (σB,σpost) where σB≡σpost (Corollary J.2), every wait-for edge in WFGpost is also present in the source-level WFGB. (Equivalently, WFGpost⊆WFGB.) This holds for mixed WFGs containing edges via both buffered channels (B(c)>0) and rendezvous channels (B(c)=0).
Proof: Since σB≡σpost, every process P is at the same abstract program point and has the same relevant guard truth values for its current potentially-blocking frontier (i.e., the same set of minimal guarded blocking Push/Pop operations, and the same local enabling conditions for each). Moreover, for buffered channels with B(c)>0, the channel empty/full predicate agrees between σB and σpost (Corollary J.2, clause (2c)). We show that each RTL edge transfers to the source-level WFG by case-splitting on B(c).
Case 1: Buffered channel (B(c)>0).
Consumer (Blocked Pop): Suppose P waits for Q via Popc in the RTL system on a channel c with B(c)>0. By Lemma K.1, occ(c)=0 in σpost (empty). By σB≡σpost, c is also empty in σB. Under the bounded-FIFO channel semantics, completion of P's Popc requires a complementary Pushc by Q. Hence P→Q is also an edge in WFGB.
Producer (Blocked Push): Symmetric. If P waits for Q via Pushc on a channel c with B(c)>0, Lemma K.1 gives occ(c)=B(c) (full) in σpost, hence also in σB. Completion of P's Pushc requires a complementary Popc by Q to make space. Hence P→Q is also an edge in WFGB.
Case 2: Rendezvous channel (B(c)=0).
Suppose P waits for Q via a blocking operation on a channel c with B(c)=0 in the RTL system. By the WFG edge definition (K.1), P is blocked: its local guard is true and the rendezvous channel-side enabling condition is false. For rendezvous, the channel-side enabling condition is "the complementary endpoint is enabled in the same cycle." Thus the edge P→Q in WFGpost implies that the complementary endpoint Q is not simultaneously enabled for the matching operation in σpost. Since σB≡σpost aligns both processes' control locations and the relevant guard truth values, Q is also not simultaneously enabled for the complementary rendezvous operation in σB. Therefore P is also blocked on the same rendezvous operation in σB, and (by A6) the complementary endpoint is the same unique process Q. Hence the same wait-for edge P→Q is present in WFGB.
Therefore every RTL wait-for dependency is also a source-level wait-for dependency, so WFGpost⊆WFGB. □

K.5 Theorem K.1 — Liveness Preservation
Statement: If the source-level bounded-FIFO system Sys_B is deadlock-free, then the post-HLS implementation RTL(Sys) is also deadlock-free. This theorem preserves absence of message-passing deadlock (WFG over blocking Push/Pop). SyncChannel/barrier deadlocks are treated as specification errors and are out of scope here.
Proof (by Contradiction):

1. Assume RTL(Sys) reaches a deadlocked state sigma_post.
2. Extract Cycle: By Lemma K.1, there exists a non-empty set of processes D forming a closed cycle in WFG_post.
3. Map to Source-Level Buffered Semantics: By Corollary J.2 (State Correspondence at the End of a Matched Observable Prefix), there exists a corresponding source-level state sigma_B of Sys_B such that sigma_B ≡ sigma_post.
4. Transfer Cycle: By Lemma K.2, every edge P→Q in WFG_post is also present in WFG_B. Since D is a closed SCC in WFG_post, D has no outgoing edges: for each P∈D and for every outgoing wait-for edge P→Q in WFG_post, we have Q∈D. By A6 (well-defined complementary endpoint per channel), the channel and complementary endpoint are the same at the source level, so each such outgoing edge P→Q in WFG_post corresponds to an outgoing edge P→Q in WFG_B with the same target Q∈D. Hence D has no outgoing edges in WFG_B and forms a closed wait-for cycle there as well.
5. Contradiction: This implies Sys_B is deadlocked in state sigma_B, contradicting the Source-Level Liveness Assumption (A5).
6. Conclusion: RTL(Sys) cannot deadlock. □

Implementation Note

Because the Appendix I, J, and K proofs above are parametric in B(c) ≥ 0, designers are free to instantiate *any* finite depth—zero included—on every channel without jeopardizing functional correctness or liveness, provided the environment upholds the weak fairness assumption.

Appendix L – Snooping Introduction, Implementation and Concerns

Snooping Introduction

If designs are completely latency insensitive, verification of the pre-HLS versus post-HLS models is straightforward. However, if the design contains some components such as arbiters which have latency-sensitive behavior, and if that latency-sensitive behavior is in some cases externally visible to the DUT, then verification becomes somewhat more complex. Techniques can be applied to simplify verification.

Consider a design which has an arbiter like Matchlib toolkit example 09*. The arbiter uses non-blocking PopNB() on its inputs, and blocking Push() on its output to emit the winner of the arbitration. Since the latency between the pre-HLS and post-HLS designs will differ, the order of transactions presented to the arbiter in the two scenarios will differ, and thus the order of the winners will differ. This may result in verification mismatches between the two models if the order of the winners is externally visible to the DUT.

To force the pre-HLS and post-HLS simulations to match, we can run the two designs side-by-side. We can snoop the inputs to the arbiter in the post-HLS model, and only allow the inputs to the pre-HLS

arbiter to proceed when the corresponding inputs are seen in the post-HLS model. This will force the order of the inputs to be equivalent between the pre-HLS and post-HLS models, and thus both arbiters will pick the same winners. When this technique is used, the pre-HLS simulation will be throttled by the post-HLS simulation, but the overall verification will still work properly.

Another related example involves interrupt request signals feeding into an interrupt controller within a CPU model. Typically, each interrupt request signal is a single bit sc_signal<>, indicating that an interrupt request is pending. If the requests originate from accelerator blocks that are being synthesized through HLS, then because of the latency differences between the pre-HLS and post-HLS models, the order of interrupt requests arriving at the interrupt controller will differ between the two models, and this will likely result in verification mismatches if the differences are externally visible to the DUT. To force the order of the requests to match, we snoop the requests arriving at the controller in the post-HLS model, and only then allow the requests to be seen in the pre-HLS model.

Simplified Snooping Approaches

In the snooping example directly above in which the arbiter is snooped, the entire post-HLS RTL DUT is simulated alongside the pre-HLS model to force the arbiter requests to be aligned in time. This is the most general case and assumes the input delays to the arbiter are difficult to determine via analysis.

Sometimes there are simpler cases where the input delays to the arbiter in the RTL DUT are easier to determine. For example, each input to the arbiter might arrive a fixed number of clock cycles after one of the primary inputs to the RTL DUT is pushed by the testbench. In this case, a much simpler model can be used to align the pre-HLS model with the post-HLS model. We can simply monitor the primary inputs to the pre-HLS model and then apply the fixed cycle delays to the pre-HLS arbiter inputs.

The two cases above illustrate two ends of a spectrum of possible approaches for extracting the delays from the RTL DUT. Between these two points there exist other possible approaches.

Snooping Implementation

To enable perfect matching between the pre-HLS and post-HLS system simulations, latency-sensitive global signals and latency-sensitive non-blocking message-passing operations need to be synchronized between the two simulations if their latency differences are externally visible to the DUT.

As explained earlier in this appendix, in the general case the entire post-HLS DUT RTL must be run alongside the pre-HLS system to achieve alignment. Examples of signals that need to be synchronized include global interrupt request signals (as discussed earlier in this appendix) and rdy/vld signal pairs for non-blocking operations on message-passing channels. All such synchronization signals and their corresponding handshake signals must be level-stable:

- A latency-sensitive signal s is level-stable if, once s becomes 1 in cycle t, it must remain 1 until the corresponding handshake signal h is 1 in some cycle $t' \geq t$.

Once the set of signals that need to be aligned between the two simulations is identified, the general rule to implement snooping is simple:

- For each of the pre-HLS and post-HLS simulations, make all readers of the signals see the logical AND of the values of each signal being driven in each separate simulation.

Often the post-HLS simulation will never run ahead of the pre-HLS simulation, because HLS typically only adds (rather than subtracts) latency within each process. This means that often the only signals that need to be delayed are on the pre-HLS side, and therefore the logical AND of the nets may not need to be driven on the post-HLS side. If this optimization technique is used, the logical AND of the nets should be compared with the actual value driven on the post-HLS side, and if they do not perfectly match then the optimization technique must not be used.

Snooping Concerns

The snooping technique is used to align pre-HLS and post-HLS latency-sensitive global signals and latency-sensitive non-blocking message-passing operations in cases where their latency differences are externally visible at the DUT boundary. When such a wrapper is applied, the pre-HLS model is throttled to follow the latency choices made by the post-HLS RTL, and the resulting traces at the observable interfaces are forced to agree.

Readers with a formal background may be concerned by this technique, because it appears to use the post-HLS RTL implementation to modify the behavior of the pre-HLS specification. From a formal point of view, the important observation is that the pre-HLS model is intentionally under-specified with respect to micro-timing/latency: subject to the R-rules, B-rules, weak fairness, and the happens-before relation on Σ (committed IO events; unsuccessful non-blocking polls are ε-steps), it can admit multiple ε-/latency-different executions that respect the same happens-before constraints. This is compatible with B1, which asserts that the post-HLS Σ-projected trace is unique under a fixed stimulus; the pre-HLS side may still have multiple admissible realizations that (when projected to Σ) match that unique RTL Σ-trace.

Snooping does not change what executions are allowed by the pre-HLS specification. Instead, it selects—purely for verification purposes—one admissible pre-HLS execution whose latency-sensitive events align with those observed in the RTL. In other words, the implementation is used to pick a witness execution of the specification, not to redefine the specification.

Experienced SoC architects tend to view this slightly differently, in terms of design tradeoffs and verification cost.

First, it is usually possible at the architectural level to avoid latency-sensitive behaviors entirely, for example by insisting that all communication be latency-insensitive and fully synchronized. However, the quality-of-results (QOR) costs of such designs may be unacceptable. Introducing latency-sensitive behavior—non-blocking arbiters, latency-sensitive global interrupt signals, and so on—is a deliberate choice made by the designer to meet performance, power, or area goals.

Second, in many practical systems, latency-sensitive behavior is not functionally observable at the DUT boundary under the equivalence relation ≈ with Σ instantiated to include only the DUT-boundary observables (Appendix G; Common Formal Definitions above). As an example, consider a DUT that contains a single-port RAM used to exchange data between two internal processes. An arbiter is required to control access to that RAM port, and the arbiter uses latency-sensitive non-blocking Pop

operations on its request channels. During HLS, internal latencies will change, so the order in which the arbiter sees pending requests and chooses winners may differ between the pre-HLS and post-HLS models.

In this example:

- The individual RAM read/write operations and the internal arbitration decisions are not directly visible at the DUT interface.
- Only the higher-level IO of the two processes (for example, their message-passing interfaces to the rest of the system) is externally visible.

One might initially conclude that it is necessary to snoop the arbiter's inputs to make the pre-HLS and post-HLS traces match. However, the modeling rules impose two additional constraints:

1. Weak fairness for the arbiter. The arbiter must satisfy the weak fairness assumptions, so that any request that remains pending is eventually granted in both the pre-HLS and post-HLS models.
2. Happens-before discipline on shared memory. The system must enforce a happens-before relation on shared-memory accesses, ensuring that sufficient synchronization exists between the two processes so that there are no read/write races through the RAM in either model.

Under these conditions, the different arbitration orders merely change the relative timing of internal operations and of causally independent external events. They do not change the functional ordering of causally dependent observable actions at the DUT boundary. In the terminology of Appendix G, the differences are incidental variations in latency rather than changes to the happens-before partial order, and therefore they are not considered observable differences in behavior at the DUT boundary. In such cases, snooping is not required. (See also Note 1 below).

(More precisely: the equivalence relation $\approx$ is parameterized by the chosen observable alphabet Σ. If internal functionality (such as the above RAM arbiter) uses channels/signals that are not designated observable in the chosen instantiation of Σ (see Common Formal Definitions), then mismatches on those internal actions are outside $\approx$ by construction: they are not in Σ. If those internal channels/signals are designated observable (e.g., by snooping for debug, or by expanding Σ for Appendix K deadlock analysis), then they are Σ-events and must match under $\approx$. In addition, even when B1 holds (unique post-HLS Σ-trace under fixed stimulus), the pre-HLS model may still admit multiple ε-/latency-different executions consistent with the same happens-before constraints; Corollary J.1 captures the intended quantification ("existence of a matching witness execution prefix") rather than requiring a single pre-chosen trace.)

Experienced SoC architects therefore try to avoid designs in which latency-sensitive internal behaviors leak directly into the observable behavior of the system under test, since this both complicates verification and makes RTL behavior less predictable. When they do introduce such behaviors—examples include non-blocking arbiters whose winners affect externally visible ordering, global interrupt request signals at the DUT boundary—they typically know exactly where those latency-sensitive interfaces are and can isolate them.

A useful analogy is a subsystem whose clock frequency is adjusted dynamically based on on-die temperature. As temperature changes, the externally visible behavior of the SoC can change (for example, in terms of throughput or timing of events), and designers may choose such a temperature-dependent scheme to meet overall system requirements. To verify such a system, we may wish to

compare a concrete RTL trace captured at a specific temperature profile with a higher-level reference model. To do so, the reference model must be driven with the same temperature evolution as the RTL saw. If that temperature profile is not otherwise under direct control, the simplest way to obtain it is to "snoop" the temperature as observed in the RTL trace and replay it into the reference model.
In this analogy, temperature is an external parameter of the environment rather than a fundamental part of the functional specification, but it still influences observable behavior. Snooping simply provides a mechanism to recover that parameter from the implementation when it cannot be easily prescribed a priori. Similarly, snooping of latency-sensitive IO provides a mechanism to supply implementation-specific latency choices—subject to the fairness and happens-before constraints—back to the pre-HLS specification so that the two models can be compared under a common environment.

Note 1 (Unobservable non-blocking micro-timing).
We treat non-blocking message-passing at the level of committed transfers:
• An unsuccessful PushNB/PopNB poll is an internal ε-step (no Σ-event).
• A successful PushNB/PopNB completion appears in Σ only as the corresponding committed Push_c/Pop_c event.
Assume the bounded-stutter premise (FPD/B4), the standing fairness/progress premises (B2–B3), and quiescence closure (B5). Assume also that these ε-steps do not change:
(i) which blocking Push/Pop or explicit synchronization is the process's next Σ-action in program order;
(ii) the truth of any guards relevant to enabling that next Σ-action; nor
(iii) any state that can influence the committed Σ history, including the identity of the next committed channel operation and the value/message payloads of any future committed Push_c/Pop_c events (in this process or downstream processes via transmitted values).
In particular, these ε-steps cannot create or remove any wait-for edge in the Appendix K Wait-For Graph except via a corresponding committed Push_c/Pop_c Σ-event (or an explicit synchronization Σ-event).
Then such non-blocking activity can affect only internal scheduling and cannot introduce new global deadlocks beyond those captured by the Appendix K Wait-For Graph over blocking Push/Pop operations. Under these premises, the liveness preservation result of Appendix K applies unchanged whether or not these interfaces are snooped.
Otherwise (if the design makes functionally significant decisions based on the number/pattern of failed non-blocking polls, or if ε-level polling/arbitration can change which value is later transmitted/received in any committed Push_c/Pop_c, or more generally if failed polls update state that later affects a Σ-observable outcome), then those failures are functionally observable and must either be modeled explicitly at Σ or aligned via snooping; otherwise the design is outside the observational model assumed by ≈.
Corollary (Trace-equivalence scope). Because ≈ is observational at Σ (committed IO events) and ignores ε-level micro-timing, Appendices I and J apply unchanged whenever non-blocking activity influences only ε-level scheduling and does not alter the committed Σ history (including values/payloads) or the enables/guards of the next Σ-actions. When the effects of such non-blocking or signal interfaces are externally visible, the snooping wrapper of Appendix L is required; under that wrapper, the same theorems apply to the wrapped runs because the committed Σ histories are aligned by construction.

Stress Testing Pre-HLS Models for Latency Robustness

The formal equivalence results in Appendices G–K establish that, under the scheduling rules and fairness assumptions, the post-HLS RTL is trace-equivalent to the pre-HLS model at all observable interfaces.

These results implicitly assume that the pre-HLS specification is *well-formed*: it must not rely on incidental, implementation-specific timing alignments for functional correctness. Designs that do rely on such incidental alignments fall outside the formal guarantees.

Designs that use non-blocking message-passing operations (e.g., PushNB/PopNB, ac_channel nb_read/nb_write) or latency-sensitive global signals are particularly vulnerable to this kind of fragility. For such designs, it is strongly recommended to subject the pre-HLS model to aggressive *latency stress tests* in which message and handshake latencies are varied across executions. The intent is to validate that the design behaves correctly across the range of weakly fair schedules permitted by the modeling rules, not just under one convenient execution order.

More concretely, verification should check that:

- Causal dependencies are explicit. All functionally significant "happens-before" relationships are enforced via message-passing, SyncChannel operations, or explicit handshake protocols, rather than by relying on the incidental execution order of concurrent processes. In the terminology of Appendix G, the design shall not depend on the ordering of causally independent events for correctness.
- Weak fairness does not hide latent deadlocks or starvation. The design continues to make progress under adversarial but *weakly fair* scheduling—i.e., enabled actions may be delayed arbitrarily long but not forever—consistent with the B2/B3 obligations on the scheduler and environment summarized in Appendix N.

If the pre-HLS model fails under such randomized-latency stress scenarios, then the specification itself is outside the formal model of this document: it violates the design rule that well-formed systems must not rely on the relative ordering of causally independent events. In that situation, the equivalence theorems still apply to well-formed traces, but they no longer guarantee that the "golden" specification is robust under the full range of latency variations allowed by the environment.

The Matchlib library provides practical mechanisms to automate these stress tests in pre-HLS simulation, including:

- Random stall injection on message-passing channels, to simulate variable communication delays while preserving rendezvous semantics.
- Latency and capacity back-annotation, to model specific per-channel buffer depths and delays, including the capacities B(c) chosen during HLS.

Worked examples of this methodology are provided in Catapult Matchlib examples 60* and 72*, which illustrate how to configure randomized stalls and back-annotated latencies when validating that a design remains well-formed and latency-robust.

Appendix M – Document Abstract

This document defines a precise user-level scheduling model for high-level synthesis (HLS) that enables system-level verification and debug to be carried out almost entirely on the pre-HLS SystemC model, while still permitting aggressive RTL optimizations in the synthesized design. It introduces a small set of uniform rules governing three classes of I/O operations—message-passing channels, signal I/O, and

explicit synchronization—and organizes them into a “basic conceptual model” that preserves source-order synchronization, pins signal reads and writes to their nearest synchronization points, and constrains the reordering of message-passing operations so that HLS cannot introduce new deadlocks.

These rules are then extended to pipelined loops, shared and external memories (via an explicit array-access mapping layer and conflict-free reordering), and “direct input” pragmas that allow stable or periodically synchronized signals to bypass unnecessary internal storage while maintaining equivalence between pre- and post-HLS behavior.

The methodology is latency-insensitive by construction but accommodates latency-sensitive islands such as cycle-accurate transactors, non-blocking arbiters, and one-way handshake protocols through encapsulation and carefully specified synchronization schemes. The document also provides concrete modeling guidelines (e.g., rules for placing signal reads/writes around wait statements, coding of rolled loops with signal I/O, and use of Matchlib Connections and SyncChannel) that allow digital verification engineers to write a single testbench in SystemVerilog UVM or SystemC/C++ and reuse it across both pre-HLS and post-HLS models with “no surprises.”

A major contribution is the formalization, in Appendix G and subsequent appendices, of a trace-equivalence relation between the pre-HLS source model and the post-HLS RTL, expressed as partial-order constraints on observable I/O actions and encapsulated in equivalence rules E1–E5. For channels whose RTL implementations introduce finite buffering, the correspondence is stated against a source-level bounded-FIFO interpretation SysB whose capacities B(c) match RTL(Sys); the rendezvous case B(c)=0 is recovered as a special case.

These proofs are compositional (per process and system-level), incorporate weak fairness and bounded-FIFO assumptions, and cover key HLS transformations including loop pipelining, added FSM states, memory-access reordering, and configurable channel buffering. Collectively, the scheduling rules, coding guidelines, and formal guarantees provide a tool-agnostic, Catapult-compatible foundation for industrial HLS use and a concrete starting point for standardization efforts within bodies such as the Accellera Synthesis Working Group.

Keywords:
High-level synthesis (HLS); SystemC; scheduling rules; latency-insensitive design; message-passing channels; signal I/O; loop pipelining; direct input pragmas; shared memory; trace equivalence; formal verification; bounded FIFOs; Catapult HLS; Matchlib; Accellera Synthesis Working Group.

Appendix N - Scheduler and Environment Fairness Assumptions

The formal results in Appendices I–K rely on several semantic assumptions about the post-HLS scheduler and its environment:

- B2 (Weak fairness of the scheduler). If the enabling predicate for an action (Push, Pop, Sync) remains continuously true from some cycle onward, the scheduler must eventually select that action within a finite, but unspecified, number of cycles.

- B3 Channel Progress Invariants (ready/valid form).
  For every channel c with capacity B(c), interpret "continuously enabled" in terms of continuous request, not as an immediate commit.
  (No deassert-before-commit assumption.) For blocking Push_c/Pop_c transfers, these requests are non-withdrawable: once asserted for a transfer attempt, they are not deasserted prior to the corresponding commit (and Push_c payload remains stable while vld_c is asserted).
  Let vld_c denote the producer's persistent request to transfer (e.g., valid=1 with a stable payload for a Push_c), and let rdy_c denote the consumer's persistent request to transfer (e.g., ready=1 for a Pop_c).
  • P_push(c): If vld_c remains asserted continuously from some cycle t_o onward while the channel is full (occ_c = B(c)), and the complementary endpoint process continuously requests the matching Pop_c (i.e., rdy_c remains asserted continuously, with the Pop_c local guard remaining true), then some Pop_c commit must eventually occur (i.e., the full condition is eventually discharged). Equivalently: when both endpoints continuously request the transfer, the system cannot remain stuck forever in the full state without a Pop_c commit.
  • P_pop(c): If rdy_c remains asserted continuously from some cycle t_o onward while the channel is empty (occ_c = 0), and the complementary endpoint process continuously requests the matching Push_c (i.e., vld_c remains asserted continuously with stable payload, with the Push_c local guard remaining true), then some Push_c commit must eventually occur (i.e., the empty condition is eventually discharged). Equivalently: when both endpoints continuously request the transfer, the system cannot remain stuck forever in the empty state without a Push_c commit.
  (For B(c)=0 rendezvous channels: if both endpoints continuously request the transfer from some cycle t_o onward (both requests persistent; guards remain true), then the rendezvous completion eventually occurs.)
  These obligations rule out "permanent back-pressure loops" that are logically independent of the local R-rules.
- B5 (System quiescence closure). If at some cycle no observable actions are enabled in any process, then within a bounded number of cycles the system reaches a fixed point and executes no further ε-steps. This prevents a dead, all-disabled state from being hidden behind an infinite tail of internal activity.

These B-rules are assumptions on the execution environment, not guarantees automatically provided by the HLS tool. In practice they place concrete requirements on arbiters, back-pressure, and external masters that interact with the post-HLS RTL.

Priority arbiter example: fair vs unfair priority

Consider a simple two-input priority arbiter inside the post-HLS RTL. Each input is driven by a message-passing channel; the arbiter issues Pop operations to select which request to serve in each cycle.

- Input 0: high-priority channel c_high
- Input 1: low-priority channel c_low

Both channels may have pending requests at the same time.

1. Fair priority arbiter (satisfies B2 / B3).

A fair implementation might still give c_high strict priority in *individual* decisions, but it ensures that a continuously pending c_low request cannot starve. In RTL terms, this can be realized by, for example:

- A round-robin or rotating-priority arbiter that periodically moves the "highest" priority to the next requester, or
- A bounded-burst priority scheme in which c_high may win at most N consecutive cycles while c_low is requesting; after that, the next grant is forced to c_low.

Under these implementations:

- If Pop_low's enable remains true indefinitely (the low-priority channel has a pending request and downstream space is available), the scheduler must eventually grant Pop_low. This satisfies B2 for that action.
- If the low-priority FIFO is full and keeps requesting service, the system ensures that some Pop_low eventually fires, discharging data and freeing space. This is consistent with P_push/P_pop in B3.

Intuitively, the arbiter is still "priority-based," but its micro-architecture ensures that every continuously enabled requester is eventually served.

2. Unfair priority arbiter (violates B2 / B3).

A more naive design might implement:

```
if (req_high) grant_high();
else if (req_low) grant_low();
```

combined with an environment in which req_high can remain asserted indefinitely. In this case, even if req_low is also continuously asserted:

- Pop_low's enabling predicate is true forever, but it is never chosen by the scheduler.
- Low-priority requests can starve indefinitely, even though they are logically ready to fire.

This behavior violates B2 (weak fairness of the scheduler). If c_low's FIFO is full and the only way to make space is to service it, permanent starvation also violates B3's progress expectations for that channel.

In such a design, the safety properties E1–E5 may still hold (trace-equivalence on actions that *do* occur), but the liveness/results that depend on B2/B3—especially the starvation-vs-deadlock arguments in Appendix K—no longer apply.

Patterns that typically satisfy the fairness assumptions

The following design patterns normally satisfy B2 and are compatible with B3/B5, provided the rest of the system is well-behaved:

- Round-robin or rotating-priority arbiters. Any requester that remains enabled will eventually be at the front of the rotation and will be granted.
- Age-based or credit-based arbiters. Requesters accumulate age or credits while waiting; the arbiter prefers older or more-starved requests, guaranteeing that long-pending actions eventually win.
- Bounded-burst fixed priority. Fixed priority is combined with a counter that limits how long a higher-priority requester can dominate while lower-priority requesters are pending. After the burst limit is reached, lower-priority requests are forced to win until the system is "caught up."
- Back-pressure with bounded stall. When ready/valid or similar handshake signals are used, the design (or its environment) must enforce that ready cannot remain low forever while valid remains high, and vice versa. For example:
  - Downstream consumers are required (by specification) to service queues at least once every N cycles when data is present.
  - External bus masters are configured such that they cannot indefinitely defer reading from full DUT FIFOs that are logically part of the interface contract.
- Clock-gating and power-management schemes that respect B5. Once no observable actions are enabled, the design either:
  - Quietly stabilizes (no further internal toggling), or
  - Explicitly enters a low-power state from which it only wakes when some observable action again becomes enabled.

In each case, the intent is the same: continuous enable implies eventual service, and once nothing is enabled, the system converges rather than oscillating internally.

Patterns that tend to violate the fairness assumptions
Conversely, the following patterns are likely to break B2/B3/B5 and therefore fall outside the scope of the liveness arguments in this document:

- Pure fixed-priority arbitration with unbounded high-priority traffic. A static priority tree with no rotation or aging, combined with workloads in which a high-priority master can keep its request asserted indefinitely, can starve lower-priority channels forever.
- "Best-effort" external masters with no progress guarantee. For example:
    - A software driver that reads from a DUT output FIFO only when it happens to poll, and that may be pre-empted indefinitely by higher-priority threads.
    - An external bus or DMA engine that is architecturally allowed to ignore some requesters forever if higher-priority traffic remains heavy.
      Such environments can violate P_push/P_pop by allowing FIFOs to remain full or empty indefinitely while the DUT is continuously requesting progress.
- Circular back-pressure loops with no escape. Two or more processes form a cycle in which each is waiting for the other's channel to change state, and no other process can break the cycle. Without an explicit design-level guarantee that some process in the loop will eventually act (for example, by dropping priority or issuing a compensating Pop/Push), B3 is not satisfied.
- Internal oscillation without quiescence. A scheduler or control FSM that can toggle internal ε-level state forever, even after all observable actions are disabled, violates B5. While such designs are uncommon in practice, patterns involving mis-configured clock gating, asynchronous feedback, or "keep-alive" timers that never expire can have this effect.

In all these cases, the trace-equivalence theorems still describe what happens when actions do occur, but the liveness claims that depend on B2/B3/B5 (for example, "a continuously enabled channel will not starve") are no longer guaranteed. Designers and verification engineers should therefore either:

- Architect their arbiters and environments to satisfy these B-rules, or
- Treat the liveness guarantees in Appendix K as *out of scope* for those particular interfaces, and rely only on the safety-oriented parts of the model.

Appendix O - Support for Multiple Clock Domains

To lift the single-clock formalism of Appendices G–K to a multi-clock setting, we model each clock domain *d* as its own synchronous island with a local cycle counter *clk_d* and apply the existing R- and E-rules unchanged to processes within a fixed domain, interpreting *clk(.)* as *clk_d(.)* for all local synchronization, signal I/O, and message-passing events. All inter-domain communication is required to go through explicit clock-domain-crossing FIFOs; at the abstraction level of Appendix G, each such CDC FIFO is just another bounded channel with capacity *B(c)* and standard ready/valid semantics, so rendezvous pre-HLS channels and buffered post-HLS channels still satisfy FIFO legality (E4), occupancy invariants, and progress obligations *P_push(c)* and *P_pop(c)*, independent of the relative phasing of the two clocks. System behavior and liveness are then expressed in terms of the existing happens-before partial order over observable actions: intra-domain edges are ordered by the local *clk_d*, while each successful Push/Pop pair on a CDC FIFO induces a cross-domain happens-before edge. The weak-fairness and progress assumptions (B2/B3) are strengthened to require fairness of each local scheduler and of each CDC synchronizer, and Appendix K's wait-for-graph and occupancy arguments are applied to this

partial order rather than to a single total clock order, so the deadlock-preservation and trace-equivalence properties (E1–E5) continue to hold provided that no raw signals cross clock domains and every cross-domain path uses a CDC FIFO whose implementation is metastability-safe but otherwise abstracted as an ordinary bounded channel.

Appendix P - AI Discussion of Alternative Formal Frameworks

The following links provide an AI discussion of alternative formal frameworks compared to the one presented in this document:

https://gemini.google.com/share/e36f154864a9

https://chatgpt.com/share/69457119-ec30-8006-8684-9a2a8b19f96f