Formal Refinement Checking in a System-level Design Methodology

Jean-Pierre Talpin, Paul Le Guernic, Sandeep Shukla, Frédéric Doucet, R.K. Gupta

To cite this version:

Formal Refinement Checking in a System-level Design Methodology

Jean-Pierre Talpin
INRIA-IRISA

Sandeep Kumar Shukla
Virginia Tech

Rajesh Gupta
University of California at San Diego

Abstract. Rising complexity, increasing performance requirements, and shortening time-to-market demands necessitate newer design paradigms for embedded system design. Such newer design methodologies require raising the level of abstraction for design entry, reuse of intellectual property blocks as virtual components, refinement based design, and formal verification to prove correctness of refinement steps. The problem of combining various components from different designers and companies, designed at different levels of abstraction, and embodying heterogeneous models of computation is a difficult challenge for the designer community today. Moreover, one of the gating factors for widespread adoption of the system-level design paradigm is the lack of formal models, method and tools to support refinement. In the absence of provably correct and adequate behavioral synthesis techniques, the refinement of a system-level description towards its implementation is primarily a manual process. Furthermore, proving that the implementation preserves the properties of the higher system-level design-abstraction is an outstanding problem.

In this paper, we address these issues and define a formal refinement-checking methodology for system-level design. Our methodology is based on a polychronous model of computation of the multi-clocked synchronous formalism SIGNAL. This formalism is implemented in the POLYCHRONY workbench. We demonstrate the effectiveness of our approach by the experimental case study of a SPECC modeling example. First, we define a technique to systematically model SPECC programs in the SIGNAL formalism. Second, we define a methodology to compare system-level models of SPECC programs and to validate behavioral equivalence relations between these models at different levels of abstraction. Although we use SPECC modeling examples to illustrate our technique, our methodology is generic and language-independent and the model that supports it conceptually minimal by offering a scalable notion and a flexible degree of abstraction.
1. Introduction

Rising complexity and performances, shortening time-to-market demands, stress high-level embedded system design as a prominent research topic. Ad-hoc design methodologies, that lifts modeling to higher levels of abstraction, the concept of intellectual property, that promotes reuse of existing components, are essential steps to manage design complexity, gain performance, accelerate design cycle. However, the issue of compositional correctness arises with these steps. Given components from different manufacturers, designed at different levels of abstraction and with heterogeneous models of computation, combining them in a correct-by-construction manner is a difficult challenge.

A gating factor for widespread adoption of the system-level design paradigm is a lack of formal models, method and tools to support refinement. In the absence of adequate behavioral synthesis techniques, the refinement of a system-level description toward its implementation is primarily a manual process. Furthermore, proving that the implementation preserves the properties of the higher system-level design abstraction is an unsolved problem.

In this aim, system design based on the so-called “synchronous hypothesis” [5] consists of abstracting the non-functional implementation details of a system away and let one benefit from a focused reasoning on the logics behind the instants at which the system functionalities should be secured. From this point of view, synchronous design models and languages provide intuitive models for integrated circuits. This affinity explains the ease of generating synchronous circuits and verify their functionalities using compilers and related tools that implement this approach.

In the relational model of the POLYCHRONY workbench [28], this affinity goes beyond the domain of purely synchronous circuits to embrace the context of globally asynchronous locally synchronous (GALS) architectures. The unique features of this model are to provide a scalable capability to describe partially clocked specifications or multi-clocked architectures and to support a formal notion of design refinement, from the early stages of requirements specification, to the later stages of deployment and synthesis, using formal verification.

We address the issue of conformance checking in system design by considering the polychronous model of computation of the POLYCHRONY workbench to define a formal refinement-checking methodology. Our approach builds upon previous work on the multi-clocked synchronous paradigm of SIGNAL [7] and verification using the related model-checking tool SIGALI [24] (the POLYCHRONY workbench). We put the polychronous model of computation [22] to work in the context of emerging high-level design languages such as SPECC [15] by the study of refinement relations between system design levels in SPECC (Figure 1).
Outline This paper is organized as follows. We start with an overview of the polychronous model of computation in Section 2. In Section 3, we provide an informal introduction to the SIGNAL data-flow notation of the POLYCHRONY workbench. Starting from this presentation, Section 4 develops a methodology aimed at checking design refinement relations correct within the POLYCHRONY workbench by introducing a suitable notion of flow-preservation. This model and methodology are put to work in Section 5 in the context of system design using SPECC. A simple design example of an even-parity checker (EPC) is used as a vehicle to explain our methodology. We outline a technique to automatically derive a model of SPECC specifications in the POLYCHRONY workbench and apply our methodology to checking the refinement of the EPC correct from its specification level design to its RTL-level design. This exercise demonstrates the capability of POLYCHRONY to support high-level design transformations operated on SPECC programs with the validation services offered by the POLYCHRONY workbench.

2. A Polychronous Model of Computation

We start with a brief overview of the polychronous model of computation, proposed in [22]. The polychronous model of computation consists of a domain of traces and of semi-lattice structures that render synchrony and asynchrony using timing equivalence relations: clock equivalence relates traces in the synchronous structure and flow equivalence relates traces in the asynchronous structure.

Domain of polychrony We consider a partially-ordered set $(T, \leq, 0)$ of tags. A tag $t \in T$ denotes a symbolic period in time. The relation $\leq$ denotes a partial order. Its minimum is noted 0. We note $C \in C$ a (possibly infinite) chain of tags. Events, signals, behaviors and processes are defined as follows:

Definition 2.1. (polychrony)
- An event $e \in E = T \times V$ is the pair of a value and a tag.
- A signal $s \in S = C \rightarrow V$ is a function from a chain of tags to a set of values.
- A behavior $b \in B$ is a function from names $x \in X$ to signals $s \in S$.
- A process $p \in P$ is a set of behaviors that have the same domain.

Figure 2 depicts a behavior $b$ over three signals named $x$, $y$ and $z$ in the domain of polychrony. Two frames depict timing domains formalized by chains of tags. Signal $x$ and $y$ belong to the same timing domain: $x$ is a down-sampling of $y$. Its events are synchronous to odd occurrences of events along $y$ and share the same tags, e.g. $t_1$. Even tags of $y$, e.g. $t_2$, are ordered along its chain, e.g. $t_1 < t_2$, but absent from $x$. Signal $z$ belongs to a different timing domain. Its tags, e.g. $t_3$, are not ordered with respect to the chain of $y$, e.g. $t_1 \nleq t_3$ and $t_3 \nleq t_1$.

![Figure 2. A behavior in the polychronous model of computation](image-url)
In the remainder, we write \( \text{tags}(s) \) and \( \text{tags}(b) = \bigcup_{x \in \text{vars}(b)} \text{tags}(b(x)) \) for the tags of a signal \( s \) and of a behavior \( b, b|_X \) for the projection of a behavior \( b \) on \( X \subseteq \mathcal{X} \) and \( b|_X = b|_{\text{vars}(b) \setminus X} \) for its complementary, \( \text{vars}(b) \) and \( \text{vars}(p) \) for the domains of \( b \) and \( p \). We write \( B|_X \) for the set of all behaviors defined on the set of variables \( X \).

Synchronous composition is noted \( p \mid q \) and defined by the union of all behaviors \( b \) (from \( p \)) and \( c \) (from \( q \)) which are synchronous: all signals they share, i.e. \( I = \text{vars}(p) \cap \text{vars}(q) \), are equal.

\[
\begin{align*}
\forall b \in B & \mid \forall (b, c) \in p \times q, \ I = \text{vars}(p) \cap \text{vars}(q), b|_I = c|_I \end{align*}
\]

Figure 3 depicts the synchronous composition, right, of the behaviors \( p \), left, and the behavior \( q \), middle, of two processes \( p \) and \( q \). Notice that the signal \( y \), shared by \( p \) and \( q \), must carry the same tags and the same values in both \( p \) and \( q \) in order for \( b \cup c \), right, to belong to \( p \mid q \).

\[
\begin{pmatrix}
x: & \bullet^{t_1} & \bullet & \bullet & \bullet \\
y: & \bullet^{t_1} & \bullet^{t_2} & \bullet & \bullet
\end{pmatrix}
\] \[
\begin{pmatrix}
y: & \bullet^{t_1} & \bullet^{t_2} & \bullet & \bullet & \bullet \\
z: & \bullet^{t_3} & \bullet & \bullet & \bullet & \bullet
\end{pmatrix}
\] \[
\begin{pmatrix}
x: & \bullet^{t_1} & \bullet & \bullet \\
y: & \bullet^{t_1} & \bullet^{t_2} & \bullet & \bullet
\end{pmatrix}
\]

Figure 3. Synchronous composition of \( b \in p \) and \( c \in q \)

**Scheduling structure** To render constraints between the occurrence of events during a period \( t \), we refine the domain of polychrony with a scheduling relation. Figure 4 depicts a scheduling relation superimposed to the signals \( x \) and \( y \) of Figure 2. The relation \( y_{t_1} \rightarrow x_{t_1} \) denotes a scheduling constraint: \( y \) should be calculated before \( x \) at the period \( t_1 \).

\[
\begin{pmatrix}
x: & \bullet^{t_1} & \bullet & \bullet & \bullet \\
y: & \bullet^{t_1} & \bullet^{t_2} & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet
\end{pmatrix}
\]

Figure 4. Scheduling relations between simultaneous events

The pair \( x_t \) of a time tag \( t \) and of a signal name \( x \) renders the date \( d \) of the event occurring at the symbolic period \( t \) along the signal \( x \). The tag \( t \) represents the period during which multiple events take place to form a reaction. It corresponds to an equivalence class between dates \( d \), as in the synchronous structures [27].

**Definition 2.2. (scheduling relation)**

The scheduling relation \( \rightarrow_b \) is a pre-order defined on dates \( D = \mathcal{X} \times T \) for a behavior \( b \) which satisfies:

\[
\forall b \in B, \forall x \in \text{vars}(b), \forall t, t' \in \text{tags}(b(x)), t < t' \Rightarrow x_t \rightarrow^b x_{t'} \land x_t \rightarrow^b x_{t'} \Rightarrow \neg(t' < t)
\]

When no ambiguity is possible on the identity of \( b \) in \( x \rightarrow^b y \), we write it \( x \rightarrow y \). A scheduling relation is implicitly transitive (\( x_t \rightarrow^b y_{t'} \rightarrow^b z_{t''} \) implies \( x_t \rightarrow^b z_{t''} \)) and its closure for restriction \( b/\mathcal{X} \) is defined by \( x_t \rightarrow^{b/\mathcal{X}} y_{t'} \) iff \( x_t \rightarrow^b y_{t'} \) and \( x, y \notin \mathcal{X} \).
Synchronous structure  Building upon the domain of polychrony, we define the semi-lattice structure which relationally denotes synchronous behaviors. The intuition behind this relation is depicted figure 5. It is to consider a signal as an elastic with ordered marks on it (tags). If the elastic is stretched, marks remain in the same relative and partial order but have more space (time) between each other. The same holds for a set of elastics: a behavior. If elastics are equally stretched, the order between marks is unchanged. In the figure 5, the time scale of $x$ and $y$ change but the partial timing and scheduling relations are preserved. Stretching is a partial-order relation which defines clock equivalence (definition 2.3).

![Figure 5. Relating synchronous behaviors by stretching.](image)

**Definition 2.3. (clock equivalence)**

A behavior $c$ is a stretching of $b$, written $b \leq c$, iff $\text{vars}(b) = \text{vars}(c)$ and there exists a bijection on tags $f$ which satisfies

$$\forall t, t' \in \text{tags}(b), t \leq f(t) \land (t < t' \Leftrightarrow f(t) < f(t'))$$

$$\forall x, y \in \text{vars}(b), \forall t \in \text{tags}(b(x)), \forall t' \in \text{tags}(b(y)), t_x \rightarrow_b t'_y \Leftrightarrow f(t)_x \rightarrow_c f(t')_y$$

$$\forall x \in \text{vars}(b), \text{tags}(c(x)) = f(\text{tags}(b(x))) \land \forall t \in \text{tags}(b(x)), b(x)(t) = c(x)(f(t))$$

$b$ and $c$ are clock-equivalent, written $b \sim c$, iff there exists a behavior $d$ s.t. $d \leq b$ and $d \leq c$.

Asynchronous structure  The asynchronous structure of polychrony is modeled by weakening the clock-equivalence relation to allow for comparing behaviors w.r.t. the sequences of values signals hold regardless of the time at which they hold these values. The relaxation relation allows to individually stretch the signals of a behavior in a way preserving scheduling constraints. Relaxation is a partial-order relation which defines flow-equivalence (definition 2.4). Two behaviors are flow-equivalent iff their signals hold the same values in the same order.

**Definition 2.4. (flow equivalence)**

A behavior $c$ is a relaxation of $b$, written $b \sqsubseteq c$, iff $\text{vars}(b) = \text{vars}(c)$ and, for all $x \in \text{vars}(b)$, $b|_{\{x\}} \leq c|_{\{x\}}$, $b$ and $c$ are flow-equivalent, written $b \approx c$, iff there exists a behavior $d$ s.t. $d \sqsubseteq b$ and $d \sqsubseteq c$.

Figure 6 depicts two asynchronously equivalent behaviors related by relaxation. The first event along $x$ has been shifted (and its scheduling constraint with an initially synchronous event along $y$ lost) as the effect of delaying its transmission using e.g. a FIFO buffer.

![Figure 6. Relating asynchronous behaviors by relaxation.](image)
Asynchronous composition is noted \( p \parallel q \) and defined by considering the partial-order structure induced by the relaxation relation. The parallel composition of \( p \) and \( q \) consists of behaviors \( d \) that are relaxations of behaviors \( b \) and \( c \) from \( p \) and \( q \) along shared signals \( I = \text{vars}(p) \cap \text{vars}(q) \) and that are stretching of \( b \) and \( c \) along the independent signals of \( p \) and \( q \).

\[
p \parallel q = \{ d \in B_{\text{vars}(p) \cup \text{vars}(q)} \mid \exists (b, c) \in p \times q, d/I \geq b/I \land d/I \geq c/I \land b/I \sqsubseteq d/I \land d/I \sqsupseteq c/I \}
\]

Figure 7 depicts the asynchronous composition, right, of the behavior \( b \in p \), left, and of the behavior \( c \in q \), middle. Notice that the signal \( x \) and \( y \) are alternated in \( p \), left, and synchronous in \( q \), middle. Asynchronous composition allows for these signals to be independently stretched in both \( p \) and \( q \) in order to find a common flow in the asynchronously composed process, right.

\[
\begin{bmatrix}
  x : e^{t_1} & e^{t_3} \\
  y : e^{t_2} & e^{t_4}
\end{bmatrix}
\parallel
\begin{bmatrix}
  x : e^{t_1} & e^{t_2} \\
  y : e^{t_1} & e^{t_2} \\
  z : \bullet & \bullet & \bullet & \bullet
\end{bmatrix} =
\begin{bmatrix}
  x : \bullet & \bullet \\
  y : \bullet & \bullet \\
  z : \bullet & \bullet & \bullet & \bullet
\end{bmatrix}
\]

Figure 7. Asynchronous composition of \( b \in p \) and \( c \in q \)

3. A Polychronous Design Language

In the POLYCHRONY workbench, the polychronous model of computation is implemented by the multi-clocked synchronous data-flow notation SIGNAL [7]. It will serve as the specification formalism used for the case study of the present article.

**Core syntax and semantics**  In SIGNAL, a process \( P \) consists of the composition of simultaneous equations \( x := f(y, z) \) over signals \( x, y, z \). A signal \( x \in X \) is a possibly infinite flow values \( v \in V \) sampled at a discrete clock noted \( \overset{\cdot}{x} \).

\[ P, Q ::= x := y f z \mid P/x \mid P \parallel Q \quad \text{(SIGNAL process)} \]

In the polychronous model of computation, Section 2, the denotation of a clock \( \overset{\cdot}{x} \) is the domain of the signal associated to \( x \): a chain of tags. We note \( \llbracket P \rrbracket \) for the denotation of a process \( P \). The synchronous composition of processes \( P \parallel Q \) consists of the simultaneous solution of the equations in \( P \) and in \( Q \). The process \( P/x \) restricts the signal \( x \) to the lexical scope of \( P \).

\[
\llbracket P \parallel Q \rrbracket = \llbracket P \rrbracket \parallel \llbracket Q \rrbracket \quad \text{and} \quad \llbracket P/x \rrbracket = \llbracket P \rrbracket/x = \{ c \leq b/\{x\} \mid b \in \llbracket P \rrbracket \}
\]

An equation \( x := y f z \) denotes a relation between the input signals \( y \) and \( z \) and an output signal \( x \) by a combinator \( f \). An equation is usually a ternary and infixed relation noted \( x := y f z \) but it can in general be an \( m + n \)-ary relation noted \( (x_1, \ldots x_m) := f(y_1, \ldots y_n) \).
**Native combinators**  SIGNAL requires four primitive combinators to perform delay $x := y \texttt{init} v$, sampling $x := y \texttt{when} \neg z$, merge $x = y \texttt{default} z$ and specify scheduling constraints $x \rightarrow y \texttt{when} \neg z$, Figure 8. The equation $x := y \texttt{init} v$ initially defines the signal $x$ by the value $v$ and then by the previous value of the signal $y$. The signal $y$ and its delayed copy $x := y \texttt{init} v$ are synchronous: they share the same set of tags $t_1, t_2, \ldots$. Initially, at $t_1$, the signal $x$ takes the declared value $v$ and then, at tag $t_n$, the value of $y$ at tag $t_{n-1}$.

\[
\begin{align*}
[x \rightarrow y \texttt{when} \neg z] & = \{ b \in B | x, y, z | \forall t \in \text{tags}(b(x)) \cap \text{tags}(b(y)) \cap \text{tags}(b(z)), x_t \rightarrow y_t \} \\
[x := y \texttt{init} v] & = \{ b \in B | x, y | \text{tags}(b(x)) = \text{tags}(b(y)) = C \in C, b(x)(\min(C)) = v \} \cap C \setminus \min(C), \text{b}(x)(t) = b(y)(\text{pred}(C)(t)) \\
[x := y \texttt{when} z] & = \{ b \in B | x, y, z | \text{tags}(b(x)) = \{ t \in \text{tags}(b(y)) \cap \text{tags}(b(z)) | b(z)(t) = \text{true} \} \} \\
[x := y \texttt{default} z] & = \{ b \in B | x, y, z | \forall t \in \text{tags}(b(y)), b(x)(t) = b(y)(t) \land y_t \rightarrow x_t \land z_t \rightarrow x_t \} \\
\end{align*}
\]

Figure 8. Semantics of polychronous operators

The equation $x \rightarrow y \texttt{when} \neg z$ forces $x$ to occur before $y$ when $z$ is present. In the equation $y \rightarrow x \texttt{when} \neg z$, for instance, there is no scheduling relation required from $x$ to $y$ unless both $x, y, z$ are present, e.g. at tag $t$.

\[
\begin{array}{cccccccccc}
\text{y} & \downarrow & \text{t}_1,v_1 & \text{t}_2,v_2 & \text{t}_3,v_3 & \ldots \\
(x := y \texttt{init} v) & x & \downarrow & \text{t}_1,v & \text{t}_2,v_1 & \text{t}_3,v_2 & \ldots & (y \rightarrow x \texttt{when} \neg z) & x & \downarrow & \text{t}_1,v & \text{t}_2,v & \text{t}_3,v_3 & \ldots \\
\text{z} & \downarrow & \text{t}_1,0 & \downarrow & \text{t}_2,1 & \ldots & \text{z} & \downarrow & \text{t}_1,v_1 & \text{t}_2,v_2 & \text{t}_3,v_3 & \ldots \\
\end{array}
\]

The equation $x := y \texttt{default} z$ defines $x$ by $y$ when $y$ is present and by $z$ otherwise. If $y$ is absent and $z$ present with $v_1$ at $t_1$ then $x$ holds $(t_1, v_1)$. If $y$ is present (at $t_2$ or $t_3$) then $x$ holds its value whether $z$ is present (at $t_2$) or not (at $t_3$). The equation $x := y \texttt{when} z$ defines $x$ by $y$ when $z$ is true (and both $y$ and $z$ are present); $x$ is present with the value $v_2$ at $t_2$ only if $y$ is present with $v_2$ at $t_2$ and if $z$ is present at $t_2$ with the value true. When this is the case, one needs to schedule the calculation of $y$ and $z$ before $x$, as depicted by $y_{t_2} \rightarrow x_{t_2} \leftarrow z_{t_2}$.

**Syntax and semantics of clocks**  In SIGNAL, the presence of a value along a signal $x$ is the proposition noted $\neg x$ that is true when $x$ is present and that is absent otherwise. The syntax of clock expressions $e$ and

clock relations \( E \) is a particular subset of SIGNAL that is defined by the induction grammar of Figure 9. The clock expression \( ^\diamondsuit_x \) can be defined by the boolean operation \( x = x \) (i.e. \( y := ^\diamondsuit_x := (x = x) \)). Referring to the polychronous model of computation, it represents the set of tags at which the signal holds a value. Clock expression naturally represent control, the clock when \( x \) represents the time tags at which the boolean signal \( x \) is present and true (i.e. \( y := \text{when } x := \text{true when } x \)). The clock when not \( x \) represents the time tags at which the boolean signal \( x \) is present and false. We write \( 0 \) for the empty clock (the empty set of tags). A clock constraint \( E \) is a SIGNAL process. The constraint \( e^\diamondsuit = e' \) synchronizes the clocks \( e \) and \( e' \). It corresponds to the process \( (x := (e = e'))/x \). Composition \( E \mid | E' \) corresponds to the union of constraints and restriction \( E/x \) to the existential quantification of \( E \) by \( x \).

\[
\begin{align*}
  e & ::= ^\diamondsuit x \mid \text{when } x \mid \text{when not } x \mid e^\diamondsuit + e' \mid e^\diamondsuit - e' \mid e^\bullet e' \mid 0 \quad \text{(clock expression)} \\
  E & ::= () \mid e^\diamondsuit = e' \mid e^\diamondsuit < e' \mid x \to y \text{when } e \mid E \mid E' \mid E/x \quad \text{(clock constraint)}
\end{align*}
\]

Figure 9. Clock and scheduling constraints

Scheduling constraints are transitive and distributive w.r.t. clocks: \( x \to y \text{when } e \to y \text{when } e' \) implies \( x \to z \text{when } e^\diamondsuit e' \) and \( x \to y \text{when } e \to y \text{when } e' \) implies \( x \to y \text{when } e^\diamondsuit e' \). Each process \( P \) corresponds to a clock constraint \( E \) satisfying \([P] \subseteq [E]\) by the inference system \( P : E \) of Figure 10 (we write \( x \to y \) for \( x \to y \text{when } e \)).

\[
\begin{align*}
  x := y$init \vspace{-3mm} \quad x := y \text{when } z := y \text{when } z \quad P : E \\
  x := y \text{default } z := y \text{when } z \quad Q := E' \\
  \hline
  \quad P / x : E/x \\
  \quad P \mid Q : E \mid E'
\end{align*}
\]

Figure 10. Inference system

**Hierarchization** The clock and scheduling constraints \( E \) of a process \( P \) hold the necessary information to decide the property of endochrony [22]. The process accepts flow-equivalent inputs \( x \) and \( y \) (left). Inputs are processed by \( p \) in clock equivalent ways (middle) so as to produce the same outputs in the same order at clock-equivalent rates (right).

\[
\begin{align*}
  x := y$init \vspace{-3mm} & \quad \text{input buffer} \\
  y := \text{endochronous process } p \vspace{-3mm} & \quad \text{input buffer} \\
  \hline
  \quad \text{endochronous process } p \\
  \text{free buffer} \quad \text{endochronous process } p
\end{align*}
\]

Figure 11. Endochrony: from flow-equivalent inputs to clock-equivalent outputs
A process is said endochronous iff, given a set I \subset \text{vars}(p) of external input signals, it has the capability to reconstruct a unique synchronous behavior (up to clock-equivalence). Formally, p is endochronous iff there exists I \subset \text{vars}(p) such that \forall b, c \in p, (b|_I) \approx (c|_I) \Rightarrow b \sim c. The behavior of an endochronous process p is depicted in Figure 11.

Clock constraints determine the order \preceq in which events are processed endochronously, definition 3.1. Rule 1 defines equivalence classes for signals of equivalent clocks. Rule 2 constructs elementary partial orders relations: the clock when x is smaller than \sim x. Rule 3 defines the insertion of a partial order of maximum e_3 under a clock e \succeq e_3. The insertion algorithm, specified in [3], yields a canonical representation of the corresponding partial order by observing that there exists a unique minimum clock e' below e such that 3 holds. We write E \Rightarrow E' iff E' is a proposition that is deductible from E in the semi-lattice of clocks.

E is hierarchical iff its clock relation \preceq has a minimum, written \text{min}_E \in \text{vars}(E), so that \forall x \in \text{vars}(E), \exists y \in \text{vars}(E), y \preceq x. H is acyclic iff E \Rightarrow x \rightarrow x when e implies E \Rightarrow e''=0 (for all x \in \text{vars}(E)). In [22], we show that if P : E and if E is acyclic and hierarchical, then P is endochronous.

Definition 3.1. The partial order \preceq of E is the largest relation satisfying

1. if E \Rightarrow \sim x = \sim y then x \preceq y (and y \preceq x).
2. if E \Rightarrow \sim x = \text{when} y or E \Rightarrow \sim x = \text{when not} y then y \preceq x.
3. if y \preceq x \succeq w and H \Rightarrow \sim z = \sim y f \sim w for any f \in \{\sim +, \sim *, \sim -\} then x \preceq z.

x and y are equivalent, written x \sim y, iff x \preceq y and y \preceq x.

Example The implications of definition 3.1 can be outlined by considering a simple SIGNAL program, Figure 12, left. Process buffer implements two functionalities. One is the process current. It defines a cell in which values are stored at the input clock \sim i and loaded at the output clock \sim o. cell is a predefined SIGNAL operation defined by:

\[x := y \text{ cell } z \text{ init } v \overset{\text{def}}{=} (m := x | \$ \text{ init } v | x := y \text{ default } m | \sim x = \sim y \sim + \sim z) / m\]

The other functionality is the process alternate which desynchronizes the signals i and o by synchronizing them to the true and false values of an alternating boolean signal b.

Clock inference (Figure 12, middle) applies the clock inference system of Figure 10 to the process buffer to determine three synchronization classes. We observe that b, c_b, zb, zo are synchronous and define the master clock synchronization class of buffer. There are two other synchronization classes, c_i and c_o, that corresponds to the true and false values of the boolean flip-flop variable b, respectively. Recalling Definition 3.1, we write:

\[b \sim c_b \sim zb \sim zo \text{ and } b \preceq c_i \sim i \text{ and } b \preceq c_o \sim o\]

This defines three nodes in the control-flow graph of the generated code, Figure 12, right. At the main clock c_b, b is calculated from zb. At the sub-clock b, the input signal i is read. At the sub-clock c_o the output signal o is written. Finally, zb is determined. Notice that the sequence of instructions follows the scheduling constraints determined during clock inference.
Some more concrete syntax  In addition to the core syntax of SIGNAL presented so far, we make extensive use of process declarations and partial equations for the purpose of modeling our case study. In SIGNAL, a partial equation \( x := y f z \) when \( e \) is the partial definition of the variable \( x \) by the operation \( y f z \) at the clock denoted by the expression \( e \). The default equation \( x := \text{defaultvalue} v \) defines the value of the variable \( x \) when it is present but no corresponding partial equation \( x := y f z \) when \( e \) applies (because \( e \) is absent). Let \( x \) be a variable defined using \( n \) partial equations and a default value \( v \):

\[
x := x_1 \text{ when } e_1 | \ldots | x := x_n \text{ when } e_n | x := \text{defaultvalue} v
\]

Once parsed, the SIGNAL compiler processes this definition by first checking the clock expressions \( e_1, \ldots, e_n \) mutually exclusive and then handling the definition as the equivalent equation:

\[
x := (x_1 \text{ when } e_1) \text{ default } \ldots \text{ default } (x_n \text{ when } e_n) \text{ default } v
\]

In SIGNAL, the declaration of a process \( P \) of name \( f \), input signals \( x_1, \ldots, x_m \), output signals \( x_{m+1}, \ldots, x_n \) is noted

\[
\text{process } f = (? x_1, \ldots, x_m ! x_{m+1}, \ldots, x_n) (| P |);
\]

Once declared, process \( f \) may be called \( (y_{m+1}, \ldots, y_n) := f(y_1, \ldots, y_m) \) with its actual parameters \( y_1, \ldots, y_n \) and behave as \( P \) with \( x_{1,\ldots,n} \) substituted by \( y_{1,\ldots,n} \). A variant declaration is that of a foreign function \( f \), accessible, e.g. from a separately compiled C library. Its call can be wrapped into SIGNAL by declaring its interface and by declaring an abstraction \( E \) of its behavior (consists of scheduling and clock constraints).

\[
\text{process } f = (? x_1, \ldots, x_m ! x) \text{ spec } (| E |) \text{ pragmas } \text{C\_CODE}\"&x = f(&x_1, \ldots &x_m)\" \text{ end pragmas};
\]

4. A Refinement Checking Methodology

The definition of the polychronous model of computation [22] accurately renders the synchronous hypothesis implemented in the multi-clocked data-flow notation SIGNAL and relates it to architectures
using communication with unbounded delay. In an embedded architecture, however, the flow of a signal
usually slides from another as the result of finite delays incurred by resource-bounded protocols, e.g.
fifo buffers. In this section, we seek towards a formulation of the formal properties implied by this
practice to check correctness of a concrete design refinement methodology.

**Finite relaxation** We start from the model of a one-place fifo buffer in SIGNAL, Figure 13, which
we will use to draw the spectrum of possible timing relations considered, modelled and checked in the
context of the present case study. The processing of process fifo is decomposed into two functionalities.

- One is the process access which defines the necessary timing constraints on the input signal i and output
  signal o via the delayed value of the boolean signal b: fifo can accepts an input at the next time sample
  iff b is true.

  \[
  \text{process access} = (? i, o ! )
  \]

  \[
  (| a := \sim o \text{ default (not } \sim i) \text{ default } b |
  | b := a$1 \text{ init false } |
  | i := \text{ when } b |
  | o := \text{ when not } b |
  ) / a, b
  \]

  \[\text{process current} = (? i ! o)\]

  \[
  (| o := (i \text{ cell } \sim o \text{ init false}) \text{ when } \sim o |
  )
  \]

  \[\text{process fifo} = (? i ! o)\]

  \[
  (| \text{access}(i, o) |
  | o := \text{ current } (i) |
  )
  \]

  Figure 13. A one-place first-in first-out buffer in SIGNAL

  The other functionality of fifo is the process current of Figure 12. Figure 14 depicts the relation
  of the signals x and y and the cell m defined by the equation y := fifo(x).

  \[
  d(x) : \bullet \bullet \bullet \\
  \downarrow \downarrow \downarrow \downarrow \\
  y := \text{fifo}(x) \\
  \]

  \[
  d(m) : \bullet \bullet \bullet \rightarrow \bullet \\
  \downarrow \downarrow \downarrow \\
  d(y) = c(x) : \bullet \bullet \bullet \\
  \]

  Figure 14. Relation between events through a one-place FIFO buffer

Definition 4.1 formalizes this relation and accounts for the behavior of fifo by implying a series
of (reflexive-anti-symmetric) relations \( \equiv_N \) (for \( N > 0 \)) which yields the (series of) reflexive-symmetric
flow relations \( \approx_N \) to identify processes of same flows up to a flow-preserving first-in-first-out buffer
of size \( N \). In Definition 4.1, we write \( \text{pred}_C(t) \) (resp. \( \text{succ}_C(t) \)) for the immediate predecessor (resp.
successor) of the tag \( t \) in the chain \( C \).

**Definition 4.1. (finite relaxation)**

The behavior \( c \) is a 1-relaxation of \( x \) in \( b \), written \( b \sqsubseteq^1 c \) iff \( \text{vars}(b) = \text{vars}(c) \) and there exists \( d/m \geq b \)
such that \( d/x = c/x \) and a chain \( C = \text{tags}(d(m)) = \text{tags}(d(x)) \cup \text{tags}(c(x)) \) such that:

- \( \forall t \in C, t \in \text{tags}(d(x)) \Rightarrow d(m)(t) = d(x)(t) \)
- \( t \not\in \text{tags}(d(x)) \Rightarrow d(m)(t) = d(m)(\text{pred}_C(t)) \)
- \( t \in \text{tags}(c(x)) \Rightarrow c(x)(t) = d(m)(t) \)

and satisfying \( \forall t \in \text{tags}(c(x)) \exists t' \in \{t, \text{succ}_C(t)\}, c(x)(t') = d(x)(t) \). We write \( b \sqsubseteq_1 c \) iff \( b \sqsubseteq^1 c \) for
all \( x \in \text{vars}(b) \), and, for all \( n > 0 \), \( b \sqsubseteq_{n+1} c \) iff there exists \( d \) such that \( b \sqsubseteq_1 d \sqsubseteq_n c \).
Desynchronization  Now, recall the process buffer of Figure 12. It essentially differs from process fifo by the policy implemented by process alternate. Process alternate synchronizes i and o to the true and false values of an alternating signal b.

This guarantees the independence or exclusion between the clocks of i and o. Each tag $t'_i$ of an event along o can only happen strictly between the tags $t_i$ and $t_{i+1}$ of two consecutive events along i, i.e. $t_i < t'_i < t_{i+1}$, and vice-versa.

The relation between Definitions 4.1 and 4.2 and the implementation of fifo and buffer of Figure 13 and 15 are brought together by the following proposition. The proof of property (1) consists of formulating the four requirements of definition 4.1 by observers written in SIGNAL and of checking them against the model of fifo. Property (2) is proved by observing that all tags of i and o satisfy $t_i < t'_i$ by induction on i and that $t_i$ and $t'_i$ form two disjoint sub-chains of the domain of b.

**Definition 4.2. (desynchronization)**
The behavior $c$ is a desynchronization of $b$, written $b \sqsubseteq c$ iff $\text{vars}(b) = \text{vars}(c)$ and there exists $d \geq b$ such that, for all $x \in \text{vars}(b)$, $d(x) = (t_i, v_i)_{i \geq 0}$, $c(x) = (t'_i, v'_i)_{i \geq 0}$ and, for all $i \geq 0$, $t_i < t'_i < t_{i+1}$.

The relation between Definitions 4.1 and 4.2 and the implementation of fifo and buffer of Figure 13 and 15 are brought together by the following proposition. The proof of property (1) consists of formulating the four requirements of definition 4.1 by observers written in SIGNAL and of checking them against the model of fifo. Property (2) is proved by observing that all tags of i and o satisfy $t_i < t'_i$ by induction on i and that $t_i$ and $t'_i$ form two disjoint sub-chains of the domain of b.

**Proposition 4.1.**

(1) $\forall b \in [x := \text{fifo}(y)], [z \mapsto b(y)] \sqsubseteq_1 [z \mapsto b(x)]$

(2) $\forall b \in [x := \text{buffer}(y)], [z \mapsto b(y)] \sqsubseteq_2 [z \mapsto b(x)]$

**Formal properties**
The series of relations $(\approx_n)_{n \geq 0}$ defines a spectrum between synchrony and asynchrony that can be modeled using the SIGNAL formalism. It is hence tempting to interpret the asynchronous partial-order $\sqsubseteq$ as the (inaccessible) limit or union $\bigcup_{N \geq 0} \sqsubseteq_N$ of this series.

**Lemma 4.1.**
- $b \approx b'$ implies $b \approx_1 b'$,
- $b \approx_n b'$ implies $b \approx b'$, for all $n > 0$
- $b \approx_m b' \approx_n b''$ implies $b \approx_{m+n} b''$, for all $m$ and $n$

Instead, we focus on the largest equivalence relation that can be modeled using SIGNAL. It consists of behaviors equal up to a timing deformation performed by a finite FIFO protocol.

**Definition 4.3. (finite flow-equivalence)**

$b$ and $c$ are finitely flow-equivalent, written $b \approx^*_n c$, iff there exists $n > 0$ and $d$ s.t. $d \sqsubseteq_n b$ and $d \sqsubseteq_n c$. 

Figure 15. A desynchronization buffer in SIGNAL
We say that a process $P$ is finitely flow-preserving iff given finitely flow-equivalent inputs, it can only produce behaviors that are finitely flow equivalent. Example of finitely flow-preserving processes are endochronous processes. An endochronous process which receives finitely flow equivalent inputs produces clock-equivalent outputs.

**Definition 4.4. (finite flow-preservation)**

$p$ is finitely flow-preserving with $I \subset \text{vars}(p)$ iff \( \forall b, c \in p, (b|_I) \approx_\approx (c|_I) \Rightarrow b \approx^* c \).

A refinement-based design methodology based on the property of finite flow-preservation consists of characterizing sufficient invariants for a given model transformation to preserve flows.

**Definition 4.5. (finite flow-invariance)**

The refinement of $p$ by $q$ is finitely flow-invariant, written $p \ll^* q$, iff $I \subset \text{vars}(p) = \text{vars}(q)$ and \( \forall (b, c) \in p \times q, (b|_I) \approx_\approx (c|_I) \Rightarrow b \approx^* c \).

The property of finite flow-invariance is a very general methodological criterion. It is reflexive ($p \ll^* p$) and transitive ($p \ll^* q \ll^* r \Rightarrow p \ll^* r$) for all flow-preserving processes ($p, q, r$). For instance, it can be applied to the characterization of correctness criteria for model transformations such as protocol insertion or desynchronization.

**Verification methodology**  Property 4.1 provides all necessary elements to define an observer giving sufficient conditions for finite flow-preservation to hold and be provable by model checking. To this end, we consider the template SIGNAL process observer of Figure 16. It is parameterized by the notation $\{P, Q\}$ over two processes named $P$ and $Q$ which we want to check finitely flow-equivalent.

```
process observer = {P, Q} (? i ! o)
    (| o := fifo (P (buffer (i))) = fifo (Q (buffer (i))) |);
```

**Figure 16.** Observer function for the property of finite flow-equivalence

The observer receives an input signal $i$. This input signal is used to generate two desynchronized signals (i.e. satisfying the hypothesis $b|_i \approx c|_i$) by using the process buffer. The flows $b|_i$ and $c|_i$ are injected to $P$ and $Q$ and the outputs collected by using fifo to avoid the synchronization of the outputs performed by the comparison $=$. If the output of the observer is always true then the equality is an invariant. For the sake of simplicity, process observer is displayed Figure 16 for two processes $P$ and $Q$ that have only one input and one output signal and with a fifo buffer of length 1. Extending the observer to accept processes with $m$ inputs, $n$ outputs and a buffer of length $k$ is obtained by structural induction starting from fifo and buffer. Theorem 4.1 formalizes the implication of processobserver for refinement checking by considering flow-preserving processes $P$ and $Q$ of same cardinality i.e. $\text{vars}(P) = \text{vars}(Q)$ and $\text{in}(P) = \text{in}(Q)$.

**Theorem 4.1. (refinement checking)**

Let $P$ and $Q$ be finitely flow-preserving processes of same cardinality $m = |\text{in}(P)| = |\text{in}(Q)|$. If, for all $b \in [x := \text{observer}\{P, Q\}(y_1, \ldots y_m)]$ and, for all $t \in \text{tags}(b(x))$, $b(x)(t) = \text{true}$, then $P \ll^* Q$. 


Let \( p = [P] \) and \( q = [Q] \) be two flow-preserving processes and let \( I = \text{in}(p) = \text{in}(q) \) be the input signals. By definition of process observer, Figure 16, and by Property 4.1, we have:

\[
(1) : \forall b \in B|_I, \forall (c, d) \in p \times q, b \sqsubseteq^I c \land b \sqsubseteq^I d \Rightarrow c \approx^*_1 d
\]

By hypothesis, \( p \) and \( q \) are both finitely flow-preserving. By definition 4.4, this requires that \( c|_I \approx^*_1 d|_I \) implies \( c \approx^* d \) for all \( (c, d) \in p \times q \). Applied to (1), this hypothesis means that \( c|_I \approx^*_1 d|_I \) also implies \( c \approx^*_1 d \) for all \( (c, d) \in p \times q \). By lemma 4.1, this yields the result expected in Theorem 4.1, as \( c \approx^*_1 d \) implies \( c \approx^* d \).

5. Formal Methods for Refinement-Based Design in SPECC

The model and method presented in Sections 2 and 4 are applied to checking refinements between design abstraction-levels correct. Section 5.2 proposes a technique to automatically represent SPECC programs in the POLYCHRONY workbench. Section 5.3 applies the methodology of Section 4 to formally establish the correctness of design refinements (Figure 17). We consider a simple SPECC programming example as case study to illustrate our methodology. It demonstrate the usability of the POLYCHRONY workbench to provide the needed model, method and tool to automatically derive conditions on specifications, verifiable by static checking or model checking, and under which the refinement of a high-level specification by its lower-level implementation can be formally checked, in a manner that is independent of a particular formalism (we consider SPECC in [36], JAVA in [35], SYSTEMC in [37]).

Larger case studies applied to concrete examples (e.g. a finite input response filter and an ARM bus) are currently under way to demonstrate the capability of our technique to provide modular verification and an environment for co-simulation. In particular, modular verification is envisaged by considering the verification of a property in a system by checking it against the model of the very components that affects it while considering a static abstraction (in terms of clock and scheduling constraints) of all other components in the system under validation. Cosimulation is being investigated by considering the controller synthesis techniques provided in the POLYCHRONY workbench and with the aim of applying them to the generation of optimized and control-sensitive simulators for large SYSTEMC designs.

5.1. Refinement-Based Design in SPECC

The SPECC system-level design methodology is depicted in Figure 18. It is based on the concept of refinement: an initial system model is gradually refined through transformations performed at several
levels of abstraction: specification, architecture, communication, and implementation. System design starts with a set of requirements and constraints, both in terms of functionality and quality, possibly captured in different models of computation.

The specification level describes the system functionality in a unified way as a starting point for system synthesis. At the architecture level, the system functionality is partitioned and partitions are assigned to different components. In the process, the computational parts of the system are ordered based on execution times and a scheduling of computation on each component. At the communication level, components are refined into bus-functional representations, which accurately describe the timing of events on the wires of the busses. Finally, at the implementation level, the components are defined in terms of their register-transfer or instruction-set architecture.

![Figure 18. SPECC design methodology [15]](image)

### 5.2. Modeling SPECC Behaviors in SIGNAL

The formal grammar of SPECC programs under consideration, Table 19, is represented in static single-assignment intermediate form akin to that of the Tree-SSA package of the GCC project [34]. SSA provides a language-independent, locally optimized intermediate representation (Tree-SSA currently accepts C, C++, Fortran 95, and Java inputs) in which language-specific syntactic sugar is absent. SSA transforms a given programming unit (a function, a method or a thread) into a structure in which all variables are read and written once and all native operations are represented by 3-address instructions.
An intermediate representation  A program \( pgm \) consists of a sequence of labeled blocks \( L:blk \). Each block consists of a label \( L \) and of a sequence of statements \( stm \) terminated by a return statement \( rtn \). In the remainder, a block always starts with a label and finishes with a return statement: \( stm_1;L:stm_2 \) is rewritten as \( L;stm_1;stm_2 \). A wait is always placed at the beginning of a block: \( stm_1;wait_v;stm_2 \). Block instructions consist of native method invocations \( x = f(y^*) \), lock monitoring and branches if \( x \) goto \( L \). Blocks are returned from by either a goto \( L \), a return or an exception throw \( x \). The declaration catch \( x \) from \( L_1 \) to \( L_2 \) using \( L_3 \) that matches an exception \( x \) raised at block \( L_1 \) activates the exception handler \( L_3 \) and continues at block \( L_2 \).

We depict the structure of the SSA for a typical SPECC program by considering the core of the EPC, Figure 20. The behavior ones counts the number of bits set to 1 in a bit-array data. It consists of three blocks. The block labeled L1 waits for the lock istart before initializing the local state variable idata to the value of the input signal data and icount to 0. Label L2 corresponds to a loop that shifts idata right and adds its right-most bit to icount until termination (condition T2). Finally, in the block L3, icount is sent to the signal ocount and idone is unlocked before going back to L1.

Translation algorithm  The function \( I[pgm] \), Table 22, implements the translation from SSA to SIGNAL. It was first developed for the JIMPLE intermediate representation of JAVA [35], then redesigned and adapted to the wider spectrum of programming languages admitting the SSA intermediate representation [34] and its used exemplified for SYSTEMC in [37].

To each block of label \( L \in \mathcal{L}_f \), the function \( I[pgm] \) associates an input clock \( x_L \) and an output clock \( x_L^{exit} \). The clock \( x_L \) is true iff \( L \) has been activated in the previous transition. The boolean signal \( x_L^{exit} \)
is true iff execution of block $L$ is terminates. The default activation condition of a block is hence $x_L$1 (equation (1) of Table 22).

For a return instruction or for a block, function $I$ returns a type $P$. For a block instruction $stm$, function $I[stm]_{L}^{e_1} = \langle P \rangle^{e_2}$ takes three arguments: an instruction $stm$, the label $L$ of the block it belongs to, and an input clock $e_1$. It returns the type $P$ of the instruction and its output clock $e_2$. The output clock of $stm$ corresponds to the input clock of the instruction that immediately follows it in the execution sequence of the block.

For instance, consider block $L_2$ of behavior ones, Figure 21. The instruction $T_1 = \text{idata}$, left, is associated with the partial equation $T_1 : = \text{idata}$1 when $L_2$1, right. It means that, if the label $L_2$ is being executed, then $T_1$ is equal to $\text{idata}$1. Next, consider instruction if $T_2 \text{ goto } L_3$. It corresponds to the partial equation $L_3 : = \text{true}$ when $T_2$. It means that control is passed to $L_3$ when $T_2$ is true. Instructions that follow are conditioned by the negative not $T_2$ to means: "in the block $L_2$ and not in its branch going to $L_3"$.

\begin{verbatim}
L2: 
T1 = idata;      | T1 : = idata1 when L2$1
T2 = T1 == 0;    | T2 : = T1 = 0 when L2$1
if T2 goto L3;   | L3 : = true when T2
T3 = icount;     | T3 : = icount$1 when not T2
...
\end{verbatim}

Figure 21. From SSA to SIGNAL

Rules (1 – 2) are concerned with the iterative decomposition of a program $pgm$ into blocks $blk$ and with the decomposition of a block into $stm$ and $rtn$ instructions. In rule (2), the input clock $e$ of the block $stm$ is passed to $stm$. The output clock $e_1$ of $stm$ becomes the input clock of $blk$.

\begin{verbatim}
(1) $I[L;blk; pgm] = I[blk]_{L}^{x_L}$1 | I[pgm] $I[stm; blk]_{L} = \text{let } \langle P \rangle^{e_1} = I[stm]_{L}^{e_1} \text{ in } P | I[blk]_{L}^{e_1}$
(3) $I[x = f(y_1...n)]_{L}^{e} = \langle E(f)(x_1...n)e \rangle^{e}$
(4) $I[if x goto L_1]_{L}^{e} = \langle y := x \text{ when } e | x_{L_1} := \text{true when } y \rangle^{e}$
(5) $I[\text{notify } x]_{L}^{e} = \langle x := \text{not } x1 \text{ when }ting e \rangle^{e}$
(6) $I[\text{wait } x]_{L}^{e} = \langle y := (x = x1) \text{ when } e | x_{L} := \text{true when } y \rangle^{e}$
(7) $I[\text{goto } L_1]_{L}^{e} = x_{L}^{e} \text{exit} := \text{true when } e | x_{L_1} := \text{true when } e$
(8) $I[\text{return } x]_{L}^{e} = x_{L}^{e} \text{exit} := \text{true when } e | x_{L}^{e} \text{exit} := \text{true when } e$
(9) $I[\text{throw } x]_{L}^{e} = x_{L}^{e} \text{exit} := \text{true when } e | x := \text{true when } e$
(10) $I[\text{catch } x \text{ from } L \text{ to } L_1 \text{ using } L_2]_{L}^{e} = x_{L_2} := \text{true when } x \text{ when } x_{L}^{e} \text{exit}
     \quad | x_{L_1} := \text{true when } x_{L_2}^{e} \text{exit}$
\end{verbatim}

Figure 22. Modeling of SSA expressions into SIGNAL

Rule (3) is concerned with the translation of native and external method invocations $x = f(y_1...n)$. 


The generic type of \( f \) is taken from an environment \( \mathcal{E}(f) \). It is given the name of the result \( x \), of the actual parameters \( y_1 \ldots n \) and of the input clock \( e \) to obtain the type of \( x = f(y_1 \ldots n) \).

For instance, Figure 23 depicts the translation of native operations in block \( L_2 \) of behavior \( \text{ones} \). The assignment of \( \text{icount} \) to the local variable \( T_3 \) is translated by the partial equation

\[
T_3 ::= \text{icount$1$ when not T2}
\]

which assigns the previous value of \( \text{icount} \) to the temporary \( T_3 \) at the clock \( \text{not T2} \) (i.e. when \( T_1 \) is not 0, Figure 21).

\[
\begin{align*}
T_3 &= \text{icount}; \\
T_4 &= T_1 \& 1; \\
\text{icount} &= T_3 + T_4; \\
\text{idata} &= T_1 \gg 1;
\end{align*}
\]

\[
\begin{align*}
T_3 &= \text{icount$1$ when not T2} \\
T_4 &= T_1 \& 1 \text{ when not T2} \\
\text{icount} &= T_3 + T_4 \text{ when not T2} \\
\text{idata} &= T_1 \gg 1 \text{ when not T2}
\end{align*}
\]

Figure 23. Translating native operations in \text{SIGNAL}

The input and output clocks of an instruction may differ. This is the case, rule (4), for an \( \text{if x goto L}_1 \) instruction in a block \( L \). Let \( e \) be the input clock of the instruction and define the fresh signal name \( y \) by the equation \( y := x \text{ when } e \). When \( y \) is false, then control is passed to the rest of the block: the output clock is not \( y \). Otherwise, the control is passed to the block \( L_1 \) at the clock \( y \). The wait-notify protocol, rules (5 – 6), is modeled using a boolean flip-flop variable \( x \). Method \text{notify}, rule (5), defines the next value of the lock \( x \) by the negation of its current value at the input clock \( e \). The \text{wait} method, rule (6), activates its output clock \( y \) iff the value of the lock \( x \) has changed at the input clock \( e \). Otherwise, control goes back to \( L \).

For example, consider the wait-notify protocol at the blocks labeled \( L_1 \) and \( L_3 \) in the \text{ones} counter. The \text{wait} instruction receives control at the clock \( x_{L_1} \). If the value of \text{istart} changes (i.e. \text{when not T0}) then \text{icount} and \text{idata} are initialized and the control is passed to the block \( L_2 \). Otherwise, at the clock \text{when T0}, a transition back to \( L_1 \) is scheduled.

\[
\begin{align*}
L_1 : \text{wait (istart)}; \\
L_3 : & \text{ocount = icount;} \\
& \text{notify (idone);} \\
& \text{goto L1;}
\end{align*}
\]

\[
\begin{align*}
T_1 &= \text{istart = istart$1$ when L1$1$} \\
L_1 &= \text{true when T1} \\
L_1b &= \text{true when not T1} \\
\text{ocount} &= \text{icount$1$ when L3$1$} \\
\text{idone} &= \text{not idone$1$ when L3$1$} \\
L_1 &= \text{true when L3$1$}
\end{align*}
\]

Figure 24. Model of wait-notify in the EPC

All return instructions, rules (7 – 9), define the output clock \( x^f_{\text{exit}} \) of the current block \( L \) by their input clock \( e \). This is the right place to do that: \( e \) defines the very condition upon which the block actually reaches its return statement. A \text{goto L}_1 \) instruction, rule (7), passes control to block \( L_1 \) unconditionally at the input clock \( e \). A \text{return} instruction, rule (8), sets the exit clock \( x_f \) to true at clock \( e \) to inform the caller that \( f \) is terminated. A \text{throw x} statement in block \( L \), rule (9), triggers the exception signal \( x \) at the input clock \( e \) by \( x ::= \text{true when } e \). The matching catch statement, of the form \text{catch x from L to L}_1 \text{ using L}_2 \) passes the control to the handler \( L_2 \) and then to the block \( L_1 \) upon termination of the handler. This requires, first, to activate \( L_2 \) from \( L \) when \( x \) is present and then to pass
control to \( L_1 \) upon termination of the handler.

**Completion** Table 22 requires all entry clocks \( x_L \) and \( x_f \) to be simultaneously present when the \( f \) is being executed. Each signal \( x_L \) holds the value \( \text{true} \) iff the block \( L \) is active during a transition currently being executed. Otherwise, \( x_L \) is set to \( \text{false} \) by \( L ::= \text{defaultvalue false} \). The same holds for local variables \( T \) with the default equation \( T ::= \text{defaultvalue T$1} \). The SIGNAL compiler guarantees the completion of the next-state logic by aggregating partial equations.

\[
\begin{align*}
L_1 & ::= \text{true when } (T_1 \text{ default } L_3$1) \text{ default false} \\
L_2 & ::= \text{true when } (L_1b$1 \text{ default not } T_3) \text{ default false} \\
L_3 & ::= \text{true when } T_3 \text{ default false} \\
L_1 & ^\neq L_2 ^\neq L_3
\end{align*}
\]

Figure 25. Completion of the next-state-logic for the EPC

The translation technique proposed in [35, 37] is modular (block-wise), conceptually simple (one equation per instruction) and language-independent (SSA is the input formalism). The host formalism, SIGNAL, supports a scalable notion and a flexible degree of abstraction. Notice that the structure of the original program is represented by program labels \( L \) which play an essential role during modeling as they represent clocks, i.e. the data-structure used by the POLYCHRONY workbench to represent the control flow of programs. This information is propagated during modeling, verification and transformation. As a result, traceability is easily provided by this information to relate an error to its original block, in addition to the name of all variables it implies.

### 5.3. A Case Study: the Even-Parity Checker

We focus on a simple SPECC programming example: an even-parity checker (EPC, figure 26), to illustrate our refinement-based methodology. We show how the specification of the EPC can be refined toward a GALS implementation with the help of the tool POLYCHRONY, showing in what respects and at which critical design stages formal methods matter for engineering its architecture. This example demonstrates the capabilities of the polychronous model of computation of SIGNAL to provide formal modeling and verification support for the capture of behavioral abstractions of high-level system descriptions.

![Functional architecture of an even-parity checker (EPC).](image)

The even-parity checker (EPC), Figure 26, consists of three functionalities: an interface thread IO, a master test thread even and a slave counting thread ones (gray elements are SPECC-specific). Numbers
are sent from IO to even via the input port In. Then, IO notifies start to even which forwards In to ones via the data port. Upon notification istart, ones counts the number of bits set to one in data and returns it to even via the ocount port. Upon notification idone, even forwards the result to IO via port Out and notifies done.

5.3.1. Specification-Level Design in SPEC

In SPEC, the design level of specification defines the functionalities and behavior of a system composed of hardware and software by means of parallel threads (called behaviors) of computations exchanging data via ports and synchronized by wait and notify events. Behavior ones, Figure 27, first waits the event istart before to load data from the input port data into the variable idata. Then, it iteratively scans idata to count the number of bits set to one in it. This is done by shifting the bits in idata right and by comparing the right-most one to 1. When the data is processed (it equals 0 and there is no more bit to shift and count) the internal count icount is returned to the ocount port and the event idone is notified. The behavior even passes values from port In to port data, notifies istart, waits idone, and returns either 0 (if ocount is odd) or 1 (it is even) along the port Out before to notify Done.

```
behavior ones (in unsigned int data, in event istart, out unsigned int ocount, out event idone) {
  void main (void) {
    unsigned int idata;
    unsigned int icount;
    while (true) {
      wait(istart);
      idata = data;
      icount = 0;
      while (idata != 0) {
        icount += idata & 1;
        idata >> 1;
      }
      ocount = icount;
      notify(idone);
    }
  }
}

behavior even (in unsigned int In, in unsigned int ocount, in event start, in event idone, out unsigned int Out, out unsigned int data, out event istart, out event done) {
  while (true) {
    wait(start);
    data = In;
    notify(istart);
    wait(idone);
    Out = ocount & 1;
    notify(done);
  }
}
```

Figure 27. Specification-level design of the EPC in SPEC.

5.3.2. Model of the Specification-Level Design in SIGNAL

Figure 28 gives a model of behavior ones in SIGNAL. It displays partial equations obtained from the translation algorithm of Figure 22. An endochronous SIGNAL program which implements the specification model of the EPC is given Appendix A. It is obtained from Figure 28 by completion of the next-state logics and by the synchronization of local variables.

In state L1, behavior ones waits for istart. It receives it at clock when not T0 and initializes idata to data, icount to 0 and steps to state L2. While in state L2 (at clock when not T2) it adds the right-most bit of idata to icount, shifts idata right and goes back to L2. If idata is zero (at
clock when T2), ones steps to L3, passes the value of icount to ocount, notifies idone and goes to L1. Process even depicts a similar decomposition of the SPECC behavior in SSA form.

```plaintext
process ones = () |
| T1 ::= istart = istart$1 when L1$1 |
| L1 ::= true when T1 |
| L2 ::= true when not T1 |
| idata ::= data$1 when L2$1 |
| icount ::= 0 when L2$1 |
| L3 ::= true when L2$1 |
| T2 ::= idata$1 when L3$1 |
| T3 ::= T2 = 0 when L3$1 |
| L4 ::= true when T3 |
| T4 ::= icount$1 when not T3 |
| T5 ::= T2 & 1 when not T3 |
| icount ::= T4 + T5 when not T3 |
| data ::= In$1 when L2$1 |
| istart ::= not istart$1 when L2$1 |
| L3 ::= true when L2$1 |
| T2 ::= idone = idone$1 when L3$1 |
| L3 ::= true when T2 |
| T4 ::= icount$1 when not T3 |
| T5 ::= T2 >> 1 when not T3 |
| icount ::= T4 + T5 when not T3 |
| data ::= In$1 when L2$1 |
| istart ::= not istart$1 when L2$1 |
| L3 ::= true when L2$1 |
| ocount ::= icount$1 when L4$1 |
| idone ::= not idone$1 when L4$1 |
| idone ::= not idone$1 when L4$1 |
| ocount ::= icount$1 when L4$1 |
| idone ::= not idone$1 when L4$1 |

process even = () |
| T1 ::= start = start$1 when L1$1 |
| L1 ::= true when T1 |
| L2 ::= true when not T1 |
| data ::= In$1 when L2$1 |
| istart ::= not istart$1 when L2$1 |
| L1 ::= true when L1$1 |
| L2 ::= true when not T1 |
| data ::= In$1 when L2$1 |
| istart ::= not istart$1 when L2$1 |
| L3 ::= true when L2$1 |
| L3 ::= true when L2$1 |
| L4 ::= true when not T2 |
| Out ::= ocount$1 & 1 when L4$1 |
| done ::= not done$1 when L4$1 |
| L1 ::= true when L4$1 |

Figure 28. Specification-level design of the EPC in SIGNAL.

5.3.3. Architecture-Level Design Refinement

The translation of the even-parity checker of Section 31 demonstrates the capability of SIGNAL to model components for specification-level SPECC designs. The typical SPECC design-flow starts with the capture of IP-blocks represented as C functions and automatic partitioning according to an appropriate cost function. After partitioning, double handshake protocols (message sequence below), or other appropriate HW-SW protocols (request-acknowledge) are inserted between the functional units.

```plaintext
unsigned int recv () {
    unsigned int rtn;
    while (!ready)
        wait (eReady);
    rtn = data;
    ack = true;
    notify (eAck);
    while (ready)
        wait (eReady);
    ack = false;
    notify (eAck);
    return rtn;
}
```

Figure 29. Implementation of a channel with double hand-shake in SPECC.
At specification-level, data exchange between the behaviors ones and even is performed by shared variables and arbitrated by a wait-notify protocol. At architecture-level, this protocol is refined by a double handshake protocol defined by the methods send and recv of the module ChMP, figure 29. The channel encapsulates the wait and notify operations performed in the specification model together with locally shared variables ack and ready.

5.3.4. Model of the Architecture Refinement in SIGNAL

The SIGNAL model of the send method, Figure 30, of the recv method, of the architecture-layer refinement of the EPC, are obtained in the very same way as for the behaviors even and ones of the specification level. The send method of the ChMP module assigns the current value of the input In to the shared variable data, sets the shared ready flag to true and waits for the notification eAck from the recv process until the shared flag ack becomes true. The same transaction is repeated to wait until the transmission of its return data to ready a new transaction.

Process send receives two parameters L1 and L7 in addition to its input data In. The boolean signal L1 is true when send receives control from its caller. The boolean signal L7 is true when send returns control to its caller. Appendix B gives the complete listing of the send and recv functionalities of the channel ChMP which were checked endochronous using the POLYCHRONY workbench to qualify for validation using our refinement checking methodology.

```plaintext
process send = (? In, L1 ! L7) |
| ready ::= false when L4$1 |
| eReady ::= not eReady$1 when L4$1 |
| data ::= In$1 when L1$1 |
| L5 ::= true when L4$1 |
| ready ::= true when L1$1 |
| T4 ::= ack$1 when L5$1 |
| eReady ::= not eReady$1 when L1$1 |
| L6 ::= true when T4 |
| T2 ::= ack$1 when L2$1 |
| L7 ::= true when not T4 |
| L3 ::= true when not T2 |
| T3 ::= eAck = eAck$1 when L6$1 |
| L4 ::= true when T2 |
| L5 ::= true when not T3 |
| T1 ::= eAck = eAck$1 when L3$1 |
| L6 ::= true when T3 |
| L2 ::= true when not T1 |
| L2, L3, L4, L5, L6, |
| ) / L2, L3, L4, L5, L6, |
| T1, T2, T3, T4; |
```

Figure 30. Model of the architecture-level channel (send method) in SIGNAL.

5.3.5. Validation of the Specification-to-Architecture Refinement

The installation of a channel between the processes even and ones incurs an additional desynchronization of the transmission between the In and Out signals. Showing that the refinement of the EPC from the specification level, process epc1, to the architecture level, process epc2, is correct requires checking that the refinement is finitely flow-invariant: epc1 ≪∗ epc2.

The verification of this property amounts to proving that, for all behaviors b and c of epc1 and epc2, flow equivalence of the input signal In, i.e. \( b|_{\text{In}} \approx c|_{\text{In}} \) implies flow equivalence of the output signal Out, i.e. \( b|_{\text{Out}} \approx c|_{\text{Out}} \).

\[
(1) : \forall b \in [\text{epc1}], \forall c \in [\text{epc2}], b|_{\text{In}} \approx c|_{\text{In}} \Rightarrow b|_{\text{Out}} \approx c|_{\text{Out}}
\]
Preliminary observations are in order to facilitate the proof of equation (1). The architecture model of the EPC only differs from the specification model by the introduction of a channel in place of a wait-notify protocol to synchronize concurrent accesses to shared variables. By contrast, the architecture model epc2 uses the double handshake protocol of the send and recv functionality of the module ChMP.

Figure 31 isolates the pattern specif that characterizes the wait-notify protocol in the specification model. The variables of the EPC models specif and archi are interfaced to signals In and Out for the purpose of verification. The producer and consumer processes prod1 and cons1 are defined by infinite loops that wrap the patterns of interest.

```plaintext
process specif = (? boolean In ! boolean Out) (
| Out := cons1() | prod1(In) |
where boolean istart init false, data init false;
process prod1 = (? In !) (
| data := In default data$1 |
| istart := not istart$1 when ^In default istart$1 |
)

process cons1 = (? ! Out) (
| T1 := istart = istart$1 when L1$1 |
| L1 := true when (T1 default L2$1) default false |
| L2 := true when not T1 default false |
| Out := data$1 when L2$1 |
| L1 ^= L2 ^= istart ^= data |
)

end;
```

Figure 31. Isolation of the synchronization protocol in the specification model

Figure 32 isolates the matching communication pattern of the architecture model wrapped in the process archi. In Figure 31, the presence of an input In triggers a wait-notify protocol that synchronizes the transmission of data from even to ones. In Figure 32, this synchronization is embedded in the call to the send and recv methods. Control to and from send and recv is provided by the labels L2 and L3. The additional label L1 closes the infinite loop.

```plaintext
process archi = (? boolean In ! boolean Out) (
| Out := cons2() | prod2(In) |
where process cons2 = (? ! Out) (
| L2 := L1$1 init true |
| Out := data$1 when L3$1 |
| L1 := true when L3$1 |
| default false |
| L1 ^= L2 ^= L3 ^= data |
| (L3, data) := recv(L2) |
|) |

process prod2 = (? In !) (
| data := In when L1$1 default data$1 |
| T1 := true when ^In when L1$1 |
| L1 := true when (not T1 default L3$1) default false |
| L2 := true when T1 default false |
| L3 := send(data$1, L2) |
| L1 ^= L2 ^= L3 ^= data |
|) |

end;
```

Figure 32. Isolation of the synchronization protocol in the architecture model

Proving equation (1) reduces to showing that the desynchronization protocol introduced by module ChMP preserves the flow of the original wait-notify protocol of the specification model. This proof is done by checking that, given desynchronized input flows $b|_{In}$ and $c|_{In}$, the specification and architecture models spec and arch provide equivalent flows along the output idata

$$\forall b \in \llbracket \text{specif} \rrbracket, \forall c \in \llbracket \text{archi} \rrbracket, b|_{In} \approx c|_{In} \Rightarrow b|_{Out} \approx c|_{Out}$$

To formulate equation (2) in the model checker SIGALI, we consider a formulation of the protocol that manipulates boolean data In and Out. This approximation still implies the expected property (2),
since neither In nor Out interfere with control in specif and archi. We obtain the formulation of the appropriate observer function (see appendix C). It is be checked invariant by SIGALI and yields the expected proof of conformance, by application of Theorem 4.1.

\[(3): \text{cqfd} := \text{observer \{specif, archi\} (In)}\]

### 5.3.6. Refinement of the Architecture Model Toward Implementation

The communication layer of the EPC, Figure 33, consists of a refinement of the data structures manipulated in the ChMP channel and of modeling (in SPEC) the behavior of the actual bus of the architecture in place of the channel abstraction ChMP. The model of the bus consists of the decomposition of the methods send and receive into sub-processes that implement the bus read and write methods.

Showing this refinement correct reduces to proving that the model of the channel’s ChMP methods send and recv are flow-equivalent to the methods read and write of the bus model. The control structure of the bus model in SIGNAL is identical to that of the channel, except for the implementation of the input/output integer signals as bit-vectors.

```plaintext
channel cBus() implements iBus {
    unsigned bit[31:0] data; cSignal ready, ack;
    void write (unsigned bit[31:0] wdata) {
        ready.assign(1);
        data = wdata;
        ack.waitval(1);
        ready.assign(0);
        ack.waitval(0);
    }
}

unsigned bit[31:0] read () {
    unsigned bit[31:0] rdata;
    ready.waitval(1);
    rdata = data;
    ack.assign(1);
    ready.waitval(0);
    ack.assign(0);
    return data;
}
```

Figure 33. Communication-level model of a bus in SPEC.

```plaintext
behavior ones(in,event,clk, ...) {
    void main(void) {
        unsigned bit[31:0] idata, icount;
        enum state {S0, S1, S2, S3} state = S0;
        while (1) {
            wait(clk);
            if (rst == 1b) state = S0;
            switch (state) {
                case S0: done = 0b;
                    if (start == 1b) state=S1
                    else state=S0;
                    break;
                case S2: icount = icount + idata & 1;
                    idata = idata >> 1;
                    if (idata == 0) state=S3
                    else state=S2;
                    break;
                case S3: outport=icount;
                    done = 1b;
                    if (ack_idone == 1b) state=S0
                    else state=S3;
                    break;
                default: done = 1b;
            }
        }
    }
}
```

Figure 34. RTL-level implementation of the EPC-core in SPEC.

Compared to the communication model of Figure 33, the RTL or implementation model of the EPC in SPEC, Figure 34, consists of a cycle-accurate implementation of the EPC that is materialized the
introduction of a master clock clk and of a reset signal rst together with the conversion of the EPC communication-layer specification into finite-state machine code. The structure of the one thread itself is close to the original one in SSA intermediate form. Each transition from a value of the state variable is guarded by an explicit synchronization to the simulation clock clk.

5.4. Conclusive Remarks

By considering a simple SpecC programming example, featuring all salient aspects of the language, we demonstrated the capability of the POLYCHRONY workbench to model the functionalities and the architecture of a system and to provide the necessary services to express model transformations and check them correct. The methodology of finite-flow invariance we employ is directly derived from previous work pertaining on the design of globally asynchronous locally synchronous architectures. The present case study departs from the very spectrum of GALS design by showing that imperative programs in the style of communicating sequential processes are equally covered. In other words, flow equivalence does not define the spectrum of architectures that are covered by our methodological principles but the very criterion for checking design refinements correct.

Naturally, other criteria can be designed and other properties checked. The POLYCHRONY workbench provides scalable abstraction of SpecC design for verification. Previous results and case studies span from the use theorem-proving [19, 25, 20] to prove properties on concrete models, model checking [6, 36] to prove properties on models abstracted by finite-state machines, static checking [26, 37] to prove properties over state-less boolean model abstractions. POLYCHRONY further provides means to optimally reuse, adapt, transform pre-defined system components and modules: hierarchization (combines several threads into one), distributed protocol synthesis (split synchronous threads into a network of communicating threads). Its current limitations are the absence of support for reasoning on dynamic resources management (memory or threads) and the lack of connexions to other models of computation (untimed, real-timed, continuous).

6. Related Works

Synchronous programming being a computational model which is popular in hardware design, and desynchronization being a technique to convert that computational model into a more general, globally asynchronous and locally synchronous computational model, suitable for system-on-chip design, one may naturally consider investigating further the links between these two models understood as Ptolemy domains [9] and study the refinement-based design of GALS architectures starting from polychronous specifications captured from heterogeneous elementary components.

Models of computation The aim of capturing both synchrony and asynchrony in a unifying model of computation is shared by several approaches: the interaction categories of Abramsky et al. in [1], the communicating sequential processes of Hoare [17] and Kahn networks [18] (communicating data-flow functions) that is one of the models supported by Ptolemy [21] and the methodology of latency insensitive protocols of Carloni et al. [10] and its extension to real-time [4]. All related models can be categorized as stratified, in the sense that they dissociate the semantics structure representing synchronous islands (the predefined pearls or IPs) from the one representing asynchrony. For instance, the heterogeneous
model of [4] is layered into a model of tag-less asynchrony and of tagged synchrony (where tags model stuttering equivalence in a way akin to clock equivalence yet without scheduling). The polychronous model of computation does not feature such a decoupling between its synchronous and asynchronous structures.

**Refinement-checking** Most of the existing formal frameworks to refinement-checking, such as B [2], Unity [11], CSP [17, 29], are essentially specification-based, in that modeling, transformation and verification are entirely envisaged within the framework of a formal notation and its companion methods and tools. By contrast, our data-flow oriented approach to refinement-checking is novel and allows us to combine a programatic approach (of SPECC) with the scalable modeling and verification techniques of the polychronous model of computation: theorem-proving [19, 25, 20], model checking [6, 36], static checking [26, 37]. Being combined to a language-independent translation technique enabling the capture of high-level system descriptions in general purpose languages such as C or JAVA, our workbench departs from specification-oriented approaches, by combining software model-checking capabilities with aggressive optimization services present in this workbench for the purpose of accelerated simulation and synthesis.

**7. Conclusions**

Until now, the refinement of a system-level description toward its implementation, in SPECC or SYSTEC was primarily envisaged as a manual process and proving conformance from the system-level abstraction to the implementation an unsolved issue. To solve it, we proposed a formal refinement-checking methodology for system-level design formalized within the polychronous model of computation of the multi-clocked synchronous formalism SIGNAL. We demonstrated the effectiveness of our approach by the experimental case study of a SPECC programming example, showing the benefits of our approach to give an accurate model of successive design abstractions of the system: functional, architecture, communication. We introduced, proved and applied a refinement-checking criterion allowing for comparing and validating behavioral equivalence relations between these successive refinements. Our methodology relies on an automated modeling technique that is conceptually minimal and supports a scalable notion and a flexible degree of abstraction. Our presentation targets SPECC yet with a generic and language-independent method. Applications of our technique range from the detection of local design errors to the compositional design refinement and conformance checking.
References


A. Listing of the Specification Model of the EPC

process epc = (? boolean start; integer In ! boolean done; integer Out)
  (| (idone, ocount) := ones (istart, data)
   | (done, Out) := even(start, In)
   |) where integer ocount init 0, data init 0;
   boolean istart init false, idone init false;

process ones = (? boolean istart; integer data ! boolean idone; integer ocount)
  (| T1 := istart = istart$1 when L1$1
   | T2 := idata$1 when L3$1 default T2$1
   | T3 := T2 = 0 when L3$1
   | T4 := icount$1 when not T3 default T4$1
   | T5 := X2(T2, 1) when not T3 default T5$1
   | L1 := true when (T1 default L4$1) default false
   | L2 := true when not T1 default false
   | L3 := true when (L2$1 default not T3) default false
   | L4 := true when T3 default false
   | idata := data$1 when L2$1 default X1(T2, 1) when not T3 default idata$1
   | icount := 0 when L2$1 default T4 + T5 when not T3 default icount$1
   | ocount := icount$1 when L4$1 default ocount$1
   | idone := not idone$1 when L4$1 default idone$1
   | idata ^= icount ^= ocount ^= idone ^= istart ^= data
   ^= L1 ^= L2 ^= L3 ^= L4 ^= T2 ^= T4 ^= T5
   |) where boolean L1 init true, L2 init false, L3 init false, L4 init false, T1, T3;
   integer idata init 0, icount init 0, T2, T4, T5; end;

process even = (? boolean start; integer In ! boolean done; integer Out)
  (| T1 := start = start$1 when L1$1
   | T2 := idone = idone$1 when L3$1
   | L1 := true when (T1 default L4$1) default false
   | L2 := true when not T1 default false
   | L3 := true when (L2$1 default T2) default false
   | L4 := true when not T2 default false
   | data := In$1 when L2$1 default data$1
   | istart := not istart$1 when L2$1 default istart$1
   | Out := X2(ocount$1, 1) when L4$1 default Out$1
   | done := not done$1 when L4$1 default done$1
   | data ^= istart ^= Out ^= done ^= L1 ^= L2 ^= L3 ^= L4
   |) where boolean L1 init true, L2 init false, L3 init false, L4 init false, T1, T2; end;

function X1 = (? i1, i2 ! i3)
  spec (| i1 ^= i2 ^= i3 | i1 --> i2 | i2 --> i3 |)
  pragmas C_CODE "&i3 = &i1 >> &i2" end pragmas;

function X2 = (? i1, i2 ! i3)
  spec (| i1 ^= i2 ^= i3 | i1 --> i2 | i2 --> i3 |)
  pragmas C_CODE "&i3 = &i1 & &i2" end pragmas;
end;
B. Listing of the Channel Model

module ChMP =
  boolean ready init false, ack init false, eReady init false, eAck init false;
  integer data init 0;

  process send = (? In, L1 ! L7)
  (| T1 := eAck = eAck$1 when L3$1 |
   T2 := ack$1 when L2$1 |
   T3 := eAck = eAck$1 when L6$1 |
   T4 := ack$1 when L5$1 |
   L2 := true when (L1$1 default not T1) default false |
   L3 := true when (not T2 default T1) default false |
   L4 := true when T2 default false |
   L5 := true when (L4$1 default not T3) default false |
   L6 := true when (T4 default T3) default false |
   L7 := true when not T4 default false |
   data := In$1 when L1$1 default data$1 |
   ready := true when L1$1 default false when L4$1 default ready$1 |
   eReady := not eReady$1 when (L1$1 default L4$1) default eReady$1 |
   L1 := L2 = L3 = L4 = L5 = L6 = L7 |
   L1 := ready = ack = eReady = eAck = data = In |
  ) where boolean L2, L3, L4, L5, L6, T1, T2, T3, T4; end;

  process recv = (? L1 ! rtn, L7)
  (| T1 := eReady = eReady$1 when L3$1 |
   T2 := not ready$1 when L2$1 |
   T3 := eReady = eReady$1 when L6$1 |
   T4 := not ready$1 when L5$1 |
   L2 := true when (L1$1 default not T1) default false |
   L3 := true when (T2 default T1) default false |
   L4 := true when not T2 default false |
   L5 := true when (L4$1 default not T3) default false |
   L6 := true when (T4 default T3) default false |
   L7 := true when not T4 default false |
   rtn := (data$1 when L4$1) default rtn$1 |
   ack := (true when L4$1) default (false when L7$1) default ack$1 |
   eAck := (not eAck$1 when (L4$1 default L7$1)) default eAck$1 |
   L1 := L2 = L3 = L4 = L5 = L6 = L7 |
   L1 := rtn = ack = eAck |
  ) where boolean L2, L3, L4, L5, L6, T1, T2, T3, T4; end;
C. Listing of the Observer Function

process observer = (? boolean In ! boolean cqfd)
(| cqfd := fifo (specif (buffer (In))) = fifo (archi (buffer (In)))
|) where

use ChMP;
use Fifo;

process specif = (? boolean In ! boolean Out)
(| Out := cons1() | prod1(In) |)
where boolean istart init false, data init false;
process cons1 = (? ! Out)
(| T1 := istart = istart$1 when L1$1
 | L1 := true when (T1 default L2$1) default false
 | L2 := true when not T1 default false
 | Out := data$1 when L2$1
 | L1 ^= L2 ^= istart ^= data
 |) where boolean L1 init true, L2, T1; end;
process prod1 = (? In !)
(| data := In default data$1
 | istart := not istart$1 when `In default istart$1
 |);
end;

process archi = (? boolean In ! boolean Out)
(| Out := cons2() | prod2(In) |)
where process cons2 = (? ! Out)
(| L2 := L1$1 init true
 | Out := data$1 when L3$1
 | L1 := true when L3$1 default false
 | L1 ^= L2 ^= L3 ^= data
 | (L3, data) := recv(L2)
 |) where boolean L1 init true, L2, L3, data; end;
process prod2 = (? In !)
(| data := In when L1$1 default data$1
 | T1 := true when `In when L1$1
 | L1 := true when (not T1 default L3$1) default false
 | L2 := true when T1 default false
 | L3 := send(data$1, L2)
 | L1 ^= L2 ^= L3 ^= data
 |) where boolean T1, L1 init true, L2, L3, data; end;
end;