SystemC\textsubscript{\textsc{fl}}: A Formalism for Hardware/Software Co-design

K.L. Man*

Abstract — SystemC\textsubscript{\textsc{fl}} is a formal language for hardware/software co-design. Principally, SystemC\textsubscript{\textsc{fl}} is the formalization of SystemC based on classical process algebra ACP. The language is aimed to give formal specification of SystemC designs and perform formal analysis of SystemC processes. This paper, designed for the first-time user of SystemC\textsubscript{\textsc{fl}}, guides the reader through modeling, analyzing and verifying designs using SystemC\textsubscript{\textsc{fl}}. This paper illustrates the use of SystemC\textsubscript{\textsc{fl}} with two case studies taken from literature.

1 Introduction

SystemC [1] is a modeling and simulation language (without formal semantics defined) based on C++ for hardware/software co-design. Recently, SystemC has received an extreme increase in industrial acceptance for system specification and simulation. The goal of developing a formal semantics is to provide a complete and unambiguous specification of the language. It also contributes significantly to the sharing, portability and integration of various applications of simulation, synthesis and formal verification. SystemC\textsubscript{\textsc{fl}} [2] is a reasonable subset of SystemC that has a rigid formal basis (i.e. formal semantics). In principle, SystemC\textsubscript{\textsc{fl}} is the formalization of SystemC based on classical process algebra (the Algebra of Communicating Processes) ACP [7]. The intended use of SystemC\textsubscript{\textsc{fl}} is for giving formal specification of SystemC designs and performing formal analysis of SystemC processes. It was shown in [3] that SystemC\textsubscript{\textsc{fl}} can be reasonably efficiently used to model software, hardware and concurrency. A key feature of SystemC\textsubscript{\textsc{fl}} is to have a single-formalism that is used to describe the various aspects of the system under consideration. Analysis/formal verification takes place by extracting simpler designs from SystemC\textsubscript{\textsc{fl}} designs that are tailored to some specific properties of interest. More precisely, various desired properties of systems/designs modeled in SystemC\textsubscript{\textsc{fl}} can be verified with existing formal verification tools by translating them formally into different formalisms that are the input languages of the existing formal verification tools. Hence, SystemC\textsubscript{\textsc{fl}} can be purportedly used for formal verification. For instance, safety properties of concurrent systems modeled in SystemC\textsubscript{\textsc{fl}} can be verified by translating those systems to PROMELA [12] that is the input language of the SPIN Model Checker [12]. Similarly, [5] reported that some desired properties of finite state systems described in SystemC\textsubscript{\textsc{fl}} can be fed into the SMV Model Checker [14] to verify them.

Also, a formal translation was defined in [4] from SystemC\textsubscript{\textsc{fl}} to a variant (with very general settings) of timed automata. The practical benefit of the formal translation from a SystemC\textsubscript{\textsc{fl}} design (describing real-time systems) to a timed automaton is to enable verification of properties of the SystemC\textsubscript{\textsc{fl}} design using existing verification tools for timed automata, such as Uppaal [13].

1.1 Related Work

The simulation semantics (including watching statement, signal assignment, and wait statement) of SystemC in the form of distributed Abstract State Machine (ASM) specifications and the Denotational Semantics for a synchronous subset of SystemC were studied by [10] and [11] respectively. It is general believed that the structured operational semantics (SOS) [8] is more intuitive [9], and the methods of ASM specifications and denotational semantics appear to be difficult to apply to describe the dynamic behavior of processes. Therefore, the language semantics of SystemC\textsubscript{\textsc{fl}} was formally defined in a standard SOS style.

1.2 Organization

The remainder of this paper is organized as follows. The next section introduces the formal language SystemC\textsubscript{\textsc{fl}}. Section 3 and 4 present some practical applications of SystemC\textsubscript{\textsc{fl}} for modeling and formal verification. Section 5 contains our conclusions.

2 SystemC\textsubscript{\textsc{fl}} Language

In this section, we introduce the formal language SystemC\textsubscript{\textsc{fl}}. For the syntax and the formal semantics of SystemC\textsubscript{\textsc{fl}}, we also refer to [2] and [6].

2.1 SystemC\textsubscript{\textsc{fl}} Data Types

In order to define the semantics of SystemC\textsubscript{\textsc{fl}} processes, we need to make some assumptions about the data types. Let \( \text{Var} \) denote the set of all variables \( \{x_0, \ldots, x_n\} \), and \( \text{Value} \) denote the set all possible values \( \{v_0, \ldots, v_m\} \) that contains at least \( \mathbb{B} \) (booleans) and \( \mathbb{R} \) (reals). A valuation is a partial function from variables to values (e.g. \( x_0 \mapsto v_0 \)). The
set of all valuations is denoted by \( \Sigma \). The set \( Ch \) of all channels and the set \( S \) of all sensitivity lists with clocks may be used in SystemC\(^{\text{FL}} \) processes that are assumed. Notice that the above proposed data types are the fundamental ones. Several extensions of data types (e.g., “sc\_bit” and “sc\_logic”) were already introduced in [3].

### 2.2 Syntax of the SystemC\(^{\text{FL}} \) Language

A process term \( P \) in SystemC\(^{\text{FL}} \) is built from atomic process terms \( AP \). SystemC\(^{\text{FL}} \) consists of various operators that operate on process terms, and it is defined according to the following grammar:

\[
AP ::= \delta \mid \text{skip} \mid x := e \mid \Delta e_n \mid \gg \gg
\]

\[
P ::= AP \mid P \triangleright b \triangleright P \mid b \Diamond P \mid P \cdot P \mid P \Theta P \mid P \sim P \mid P \bowtie P \mid P \ll P \mid \partial_H(P) \mid \tau(P) \mid \pi(P) \mid \triangleright(P)
\]

The operators are listed in descending order of their binding strength as follows: \{\triangleright, \\triangleright, \Diamond, \cdot, \Theta, \bowtie, \ll, \gg, \sim, \bowtie\}. The operators inside the braces have equal binding strength. In addition, operators of equal binding strength associate to the left, and parentheses may be used to group expressions.

Below is a brief introduction of the formal language SystemC\(^{\text{FL}} \). The formal semantics of SystemC\(^{\text{FL}} \) is given in subsection 2.3. Due to limitation of pages, deduction rules\(^1\) for operational semantics of SystemC\(^{\text{FL}} \) are not given in this paper. For those interested in more details, please read [2] and [6].

A constant called deadlock \( \delta \) is introduced, which represents no behavior. The skip process term performs the internal action \( \tau \) which is not externally visible. The assignment process term \( x := e \), which assigns the value of expression \( e \) to \( x \) (modeling a SystemC “assignment” statement). The delay process term \( \Delta e_n \) is able to delay the value of numerical expression \( e_n \). The unbounded delay process term \( \gg \) (modeling a SystemC “wait” statement) may delay for a long time that is unbounded or perform the internal action \( \tau \).

The conditional composition \( p \triangleright b \triangleright q \) operates as a SystemC “then\_if\_else” statement, where \( b \) denotes a boolean expression and \( p, q \in P \). The watching process term \( b \Diamond p \) is used to model a SystemC “watching” statement. The sequential composition \( p \cdot q \) models the process term that behaves as \( p \), and upon termination of \( p \), continues to behave as process term \( q \). The alternative composition \( p \Theta q \) models a non-deterministic choice between process terms \( p \) and \( q \). The timeout process term \( P \sim q \) (modeling a SystemC “time out” construct) behaves as \( p \) if \( p \) performs a time transition before a time \( d \in \mathbb{R}_{>0} \); otherwise, it behaves as \( q \). The watchdog process term \( p \cdot q \) behaves as \( p \) during a period of time less than \( d \), at time \( d \), \( q \) takes over the execution from \( p \). If \( p \) performs an internal cancel \( \chi \) action, then the delay is canceled, and the subsequent behavior is that of \( p \) after \( \chi \) is executed. The repetition process term \( *p \) (modeling a SystemC “loop” construct) executes \( p \) zero or more times.

The parallel composition \( p \parallel q \), the left-parallel composition \( p \bowtie q \), and the communication composition \( p \sim q \) are used to express parallelism (actions are executed in an interleaving manner, with the possibility of communication of actions). The encapsulation of actions is allowed using \( \partial_H(p) \), where \( H \) represents the set of all actions to be blocked in \( p \). The abstraction \( \tau_1(p) \) behaves as the process term \( p \), except that all actions names in \( 1 \) are renamed to the internal action \( \tau \).

The maximal progress \( \tau_1(p) \) assigns action transitions a higher priority over time transitions. This operator is needed to establish a desired communication behavior. That is, both the sender and the receiver must be able to perform time transitions, but if two of these can communicate (i.e. performing action transitions), they should not perform time transitions. The grouping of actions and executing them in one step can be done by using \( \triangleright(p) \).

Informal semantics of SystemC states that SystemC incorporates both point-to-point communication and multi-party communication mechanisms for the interaction amongst processes. However, there are no (implicit) statements in SystemC for modeling these communication mechanisms. In order to capture these facts in SystemC\(^{\text{FL}} \), operators \( \bowtie, \ll, \sim, \partial_H, \tau_1 \), and \( \pi \) are introduced to give formal specification for point-to-point communication and multi-party communication mechanisms.

### 2.3 Semantics of the SystemC\(^{\text{FL}} \) Language

**Definition 1** A SystemC\(^{\text{FL}} \) process is a quintuple \( \langle P, \Sigma, \Sigma, S, Ch \rangle \). We use the convention \( \langle p, \sigma, \sigma, s, m \rangle \) to write a SystemC\(^{\text{FL}} \) process, where \( p \) is a process term; \( \sigma, \sigma' \) are valuations; \( s \) is a sensitivity list with clocks; and \( m \) is a channel.

**Definition 2** The set of actions \( \Delta_\Sigma \) contains at least \( aa(x, v), \chi \) and \( \tau \), where \( aa(x, v) \) is the assignment action (i.e. the value of \( v \) is assigned to \( x \)), \( \chi \) is the internal cancel action and \( \tau \) is the internal action. The set \( \Delta_\Sigma \) is considered as a parameter of SystemC\(^{\text{FL}} \) and can be freely instantiated.

**Definition 3** A formal semantics for SystemC\(^{\text{FL}} \) processes is given in terms of a Labelled Transition System (LTS). We define the following transition relations on SystemC\(^{\text{FL}} \) processes:
In this section, we apply \texttt{SystemC} to give the formal specification of a case study taken from literature.

3.1 Synchronous D Flip Flop

D flip flops are one of the most basic building blocks of RTL designs. Below is a SystemC implementation that implements a synchronous D flip flop.

\begin{verbatim}
// dff.h
#include "systemc.h"
SC_MODULE(dff) {
  sc_in<int> din;
  sc_in<bool> clock;
  sc_out<int> dout;

  void doit() {
    dout = din;
  }

  SC_CTOR(dff) {
    SC_METHOD(doit);
    sensitive_pos << clock;
  }
}
\end{verbatim}

A formal \texttt{SystemCFL} specification of the above synchronous D flip flop is given as follows:

\[
\langle \text{Cond}_{\text{clock}}(\sigma', \sigma, s) \cup (d_{\text{out}} := d_{\text{in}}), \sigma', \sigma, s, m \rangle \quad \text{for some } \sigma', \sigma, s, m.
\]

\texttt{Cond}_{\text{clock}} is a function that returns true if a positive edge occurs on port clock. The formal \texttt{SystemCFL} specification of the above synchronous D flip flop has a clock input \texttt{(clock)}, a data input \texttt{(d_{in})}, and a data output \texttt{(d_{out})}. When a positive edge occurs on the clock input (which means the function \texttt{Cond}_{\text{clock}} returns true), the input port data \texttt{(d_{in})} is assigned to the output port \texttt{(d_{out})}. Notice that \texttt{clock}, \texttt{d_{in}}, \texttt{d_{out}} \in \texttt{dom}(\sigma'), \texttt{dom}(\sigma); and only \texttt{clock} \in s.

4 Purportedly Used for Formal Verification

In this section, we present the application of SPIN to verify the mutual exclusion algorithm of Dekker modeled in \texttt{SystemCFL}, by translating the \texttt{SystemCFL} design to PROMELA.

4.1 Dekker’s Mutual Exclusion

The mutual exclusion algorithm of Dekker is used by two processes (A and B) which communicate through shared variables. It is intended to prevent the processes being simultaneously entered in their critical section. Since Dekker’s Mutual Exclusion is a well-known case study of the concurrency theory, we do not further give the description and explanation of this algorithm. We only give the formal specification of it in \texttt{SystemCFL}.

In order to increase the readability, we introduce syntactic sugars for various process terms. The syntactic sugars for the process terms A and B of the mutual exclusion algorithm of Dekker are as follows:

\[
A \equiv (x := 1 \bullet t = B_1) \bullet (mu := mu + 1 \bullet mu := mu - 1 \bullet x := 0) \triangleright (y = 0) \land (tu = A_1) \triangleright \delta
\]

\[
B \equiv (y := 1 \bullet t = A_1) \bullet (mu := mu + 1 \bullet mu := mu - 1 \bullet y := 0) \triangleright (y = 0) \land (tu = B_1) \triangleright \delta
\]

Since the process terms A and B execute concurrently, the parallel composition is used to model the complete system. The complete system with initial value for variables is modeled as follows:

\[
\langle A \parallel B, \sigma', \emptyset, \emptyset \rangle \quad \text{for some } \sigma', \emptyset \in \texttt{dom} \emptyset \text{ and } \emptyset \text{ denote empty element and the undefinedness respectively.}
\]

Note that the variable \texttt{mu} is introduced as a flag. In this case study, if \texttt{mu} = 2, which indicates that process terms A and B enter simultaneously in their critical section.

Presenting the formal translation scheme from \texttt{SystemCFL} to PROMELA, and the syntax and semantics of PROMELA are far beyond the scope of this
paper, therefore we do not show them. Nevertheless, the translation of the above-given formal specification of Dekker’s Mutual Exclusion algorithm from SystemC to PROMELA model is straightforward and it is shown as follows:

```c
/*declaration*/
bit x, y;
byte t, mu;
proctype A() {
  x = 1;
  t = Bt;
  ((y == 0)||(t == At)) -> /* critical section */
  mu ++;
  mu --;
  x = 0;
}
proctype B() {
  y = 1
  t = At;
  ((x == 0)||(t == Bt)) -> /* critical section */
  mu ++;
  mu --;
  y = 0;
}
proctype monitor() {
  assert (mu != 2);
}
init {
  run A(); run B(); run monitor()
}
```

Notice that the process `monitor` is introduced and needed in the PROMELA model to check whether mutual exclusion is valid. If the condition of the assert statement (i.e., `mu != 2`) does not hold, SPIN will produce an error report. The process `init` is used to start processes.

5 Conclusions

In this paper, the main aspects of the current status of the formal language SystemCFL are presented. Then, the use of the SystemCFL through some case studies taken from literature is illustrated. Also, some practical applications of SystemCFL are shown that can be purportedly used for formal verification.

References