Interpretation of AADL Behavior Annex into synchronous formalism using SSA
Yue Ma, Jean-Pierre Talpin, Thierry Gautier

To cite this version:

HAL Id: hal-00554416
https://hal.archives-ouvertes.fr/hal-00554416
Submitted on 10 Jan 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Interpretation of AADL Behavior Annex into synchronous formalism using SSA

Yue Ma        Jean-Pierre Talpin   Thierry Gautier
INRIA, Unité de Recherche Rennes-Bretagne-Atlantique, Campus de Beaulieu, 35042 Rennes Cedex, France
Email: {Yue.Ma, Jean-Pierre.Talpin, Thierry.Gautier}@irisa.fr

Abstract

This article focuses on the essence and distinctive features of the AADL behavioral aspects, for which we use the code generation infrastructure of the synchronous modeling environment SME. It introduces an effective method for transforming a behavior specification consisting of transitions and actions into a set of synchronous equations. We present an approach for this transformation using SSA as an intermediate formalism. This interpretation minimizes introducing new state variables and transitions.

1 Introduction

Nowadays, embedded systems are an integral part of safety critical systems in various domains, such as avionics, automotive and telecommunications. Typically, they have a long life cycle of development and maintenance. In this process, architecture design and early analysis of embedded systems are two of the major challenges for designers using modeling languages such as AADL [1] (Architecture Analysis and Design Language) to describe the systems.

AADL is a language which supports the modeling of component-based systems as an assembly of software components mapped onto execution platforms. The modeling aspect of system design activity is becoming increasingly essential, since it allows prototyping and experiments without necessarily having a physical implementation of the system. The Behavior Annex is proposed as an extension of AADL to offer a way to specify the behaviors of components. AADL allows a fast design entry and software/hardware co-design. However, system validation and verification is a critical challenge. What we are seeking for is to use formal methods to ensure the quality of system designs.

Synchronous languages [4], such as Signal [2, 3], have been used successfully for the design of real-time critical applications to significantly ease the modeling and validation of software components. Their associated toolsets provide formal transformation, automatic code generation, verification, etc.

Signal is a dataflow relational language that relies on the polychronous model [3]. Signal handles unbounded series of typed values \((x_t)_{t \in \mathbb{N}}\), called signals, denoted as \(\mathbb{x}\) and implicitly indexed by the discrete pace of its clock, noted \(\hat{\mathbb{x}}\). At a given instant, a signal may be present or absent. Two signals are synchronous if they are always present (or absent) at the same instants.

In Signal, a process (written \(P\) or \(Q\)) consists of the synchronous composition (noted \(P | Q\)) of equations (written \(x := y f z\)) over signals. An equation \(x := y f z\) defines the output signal \(x\) by the result of the application of operator \(f\) to its input signals \(y\) and \(z\). In addition to the extension to signals of usual functions on values (e.g., boolean or arithmetic operations), the specific basic Signal equations are the delay \(x := y \uparrow 1\) init \(v\), the sampling \(x := y \text{ when } z\), and the merging \(x := y \text{ default } z\). The reader is referred to [3] for definitions. The process \(P|x\) restricts the lexical scope of the signal \(x\) to the process \(P\). The abstract syntax of a process \(P\) in Signal is defined as:

\[ P, Q := x := y f z | P | Q | P|x \]

Relying on these bases, we propose an approach to automatically interpret AADL Behavior Annex into the synchronous formalism Signal. We are concerned with a method to embed notations of the AADL Behavior Annex in a suitable model of computation for the purpose of formal verification and code generation. To model and compile all distinctive programming features of AADL behaviors, transitions and actions, we use the code generation infrastructure of the synchronous modeling environment SME [5]. The SME environment is a front-end of Polychrony [7] (which is a toolset for Signal) in the Eclipse environment based on Model-Driven Engineering (MDE) technologies.

The model transformation specified here relies on an inductive SSA (static single assignment) [6] transformation algorithm across transitions/actions, that produces intermediate representation. A program is said to be in SSA form whenever each variable in the program appears only once on the left hand side of an assignment. Only one new value of a variable \(x\) should at most be defined within an instant. The SSA form of a program replaces assignments of a program variable \(x\) with assignments to new versions of \(x\), uniquely indexing each assignment. The \(\phi\) operator is needed to choose the value depending on the program control-flow, where a variable can be assigned in both branches of a conditional statement or in the body of a loop. As SSA is an intermediate representation, the introduction
of the \( \phi \)-function will not consume execution cost. The
compilation will optimize the final execution code. It intro-
duces an effective method for transforming behavior spec-
fications consisting of transitions and actions into a set of
synchronous equations. This transformation minimizes the
needed state variables and component synchronization.

In this paper, we show how to not only translate the core
imperative programming features into equations, but also
extend it to the mode automata that control the activation
of such elementary transitions and actions. We give an
overview of AADL and Behavior Annex in Section 2.
The principles of the interpretation from AADL Behavior
Annex to Signal are described in Section 3. Experimental
results are provided by a case study. Some related works
and conclusions are given in Section 4 and Section 5.

2 AADL and Behavior Annex

AADL is an SAE standard aimed at high level design
and evaluation of the architecture of embedded systems.
The language employs formal modeling concepts for the
description of software and hardware architecture. It focuses
on the description of systems using the component-based
paradigm. A set of predefined components are offered:
- **Application software components** include process,
  thread, thread group, subprogram, and data components.
- **Execution platform components** model the hardware
  part of the system. This includes the processor, memory,
  device, and bus components.
- **Composite components** model components consisting
  of both hardware and software. A system component mod-
  els a component containing execution platform, application
  software and other composite components.

The AADL Behavior Annex [8] is an extension of the
core of the standard to offer a way to specify the local func-
tional behavior of the components. It supports describing
precisely the behaviors, such as port communication, com-
putation, timing, etc. A Behavior Annex can be attached to
the thread or a subprogram: threads or subprograms start
from an initial state, and a transition to a complete (resp. return)
state ends a thread (resp. subprogram). Transitions may be
guarded by conditions, and actions may be attached.

Figure 1 is a behavior specification of a *door_handler*
thread from a SDSCS (Simplified Doors and Slides Con-
control System) [9]. It comprises two transitions with an initial
state \( s_0 \) which is also a complete state. The thread will ex-
cute the transitions depending on the guarded conditions.

We will formalize the semantics of AADL behavior
annex by isolating the core syntactic categories that charac-
terize its expressive capability: transitions and actions.

**Behavior specifications** The behavior specification
defines a transition system. A behavior specification
**behavior_spec** \( x \ A \) describes system transitions from a
source state \( s \) to a destination state \( t \). A transition can be
guarded with events or boolean conditions, and actions \( S \)
can be attached. When a **behavior_spec** is first triggered, it
starts execution from an initial state, specified as \( s : \text{initial state} \), and ends with a complete (return for subprogram)
state, specified as \( t : \text{complete state (return state)} \).

![Figure 1. Behavior Annex example](image-url)

\[
\text{thread implementation} \quad \text{door_handler.imp} \\
\text{annex behavior specification} \{++
\text{states}
\begin{array}{l}
\text{s0: initial complete state;}
\text{transitions}
\begin{array}{l}
\text{s0} \cdot [(\text{on (dps > 3) and handle}) \rightarrow \text{s0} \{ \\
\text{warn_diff pres = true;}
\text{door_info = locked;}
\text{if (on ground) door_locked = false;}
\text{else door_locked = true; and if;}
\}];
\text{s0} \cdot [(\text{on not (dps > 3 and handle)}) \rightarrow \text{s0} \{
\text{warn_diff pres = false;}
\text{door_info = locked;}
\text{if (in flight) door_locked = true;}
\text{else door_locked = false; and if;}
\}];
\end{array}
\end{array}
\}
\text{end door_handler.imp;}
\]

\[
\text{behavior_spec} \quad x \ A \ \text{where} \ A \ ::= \ s_1 \rightarrow \ s_j \{ \underline{S} \} \\
\text{and} \ g ::= [(\text{on exp}) \mid \text{[when exp] \mid exp} \]
\text{and} \ s ::= (\text{initial \mid complete \mid return state})
\text{The guard} \ g \text{can be either an expression \text{exp} or contain an optional event or event data receipt \text{e} and an optional boolean condition \text{(on exp)} \text{[when exp]}.}
\text{The condition may depend on the received data, and it can be split in two parts: the \text{on} part expresses conditions over the current state, and the \text{when} part expresses a condition over the data to be read.}
\begin{itemize}
\item An event \text{e} can be a receipt from an event port \text{(p?}, or from an event data port \text{(p!(x))} where \text{x} is a state variable or a data subcomponent.
\end{itemize}

**Actions** Actions are sequences of operations on variables
that are performed during the execution of transitions.

\text{(action)} \quad S ::= x := f(y, z) \mid p? \mid p!(x) \mid p! x \mid p(x)
\text{if x then S1 else S2 for } (x \text{ in X) S}
\text{delay}(\text{min, max}) \mid \text{computation(min, max)} \mid S_1; S_2
\text{An assignment } x := f(y, z) \text{ defines the value of } x \text{ from the function } f \text{ of the current values of } y \text{ and } z.
\text{The conditional if x then S1 else S2 executes S1 if the current value of } x \text{ is true, otherwise executes S2.}
\text{The finite loop for } (x \text{ in } X) S \text{ allows iterations over finite integer ranges or over unparameterized types, which are specified by a data classifier.}
\text{The timing actions } \text{delay(min, max)} \text{ and } \text{computation(min, max)} \text{ specify non-deterministic waiting time and computation time intervals. The difference is that } \text{computation(min, max)} \text{ consumes CPU, while } \text{delay(min, max)} \text{ does not.}
The message sending or receiving actions express the communication of messages. A statement \( p! \) calls the send service on an event or event data port \( p \). The event is immediately sent to the destination with the stored data if any, \( p!(x) \) writes data \( x \) to the event data port \( p \) and calls the send service. \( p? \) dequeues an event from event port \( p \). \( p?(x) \) dequeues a data in the variable \( x \).

- Sequences of actions \( S_1; S_2 \) are executed in order.

### 3 Interpretation and semantics of AADL Behavior Annex

In this section, we will present general rules to interpret the AADL Behavior Annex into Signal. This interpretation uses SSA as an intermediate formalism. The transitions and actions are transformed into a set of synchronous equations.

In order to distinguish between the transitions of different interpretation stages, we use \( S \in \mathcal{S} \) to represent the general action in the original transition \( T \in \mathcal{T} \). \( B \in \mathcal{B} \) to represent the basic actions attached to the intermediate transition \( U \in \mathcal{U} \), and \( A \in \mathcal{A} \) to represent the SSA form actions attached to the SSA form transition \( W \in \mathcal{W} \). We introduce a notation \( \text{def} (A) := x \) referring the left hand side of an assignment \( x := f(y,z) \), and \( \text{use}(A) := f(y,z) \) referring the right hand side.

- \( \mathcal{B} \ni B := x := f(y,z) | p! | p!(x) | p! | p!(x) | B_1; B_2 \)
- \( \mathcal{S} \ni S := B \text{ if } x \text{ then } S_1 \text{ else } S_2 \text{ for } (x \in X) S \)
- \( \text{delay(min, max)} | \text{computation} | \text{min, max} \) \( S_1; S_2 \)
- \( \mathcal{A} \ni A := x := f(y,z) | A_1; A_2 \)
- \( \forall x \in \text{def}(A), x \text{ occurs at most once in } A \)

Because actions are attached to transitions, we must take into consideration the states which they depart from and enter in, when interpreting the actions. We use \( \mathcal{I}(T) \) to note the interpretation of a transition \( T \) to Signal process. The transformation \( \mathcal{I}(T) \) of the AADL transitions/actions to Signal is addressed in three steps:

- **Step 1**: \( T \xrightarrow{\mathcal{I}_x} \mathcal{U} \xrightarrow{\mathcal{I}_u} \mathcal{W} \xrightarrow{\mathcal{I}_w} \mathcal{P} \)

  - **Step 1**: \( T \xrightarrow{\mathcal{I}_x} \mathcal{U} \). Each transition \( T \in \mathcal{T} \) with attached sequence of general actions \( S \in \mathcal{S} \), is decomposed into sets of basic transitions \( U \in \mathcal{U} \), in which all the actions are basic actions \( B \in \mathcal{B} \).

  - **Step 2**: \( \mathcal{U} \xrightarrow{\mathcal{I}_u} \mathcal{W} \). For each intermediate transition \( U \in \mathcal{U} \), the basic actions \( B \in \mathcal{B} \) are depicted in SSA form \( A \in \mathcal{A} \). Each use of an original variable \( x \) is replaced by a new version, so that the actions can be executed in the same instant.

  - **Step 3**: \( \mathcal{W} \xrightarrow{\mathcal{I}_w} \mathcal{P} \). Translate the SSA form actions \( A \in \mathcal{A} \) to Signal equations.

The interpretation of transitions \( T_1 \parallel T_2 \) can be parallel:

\[
\mathcal{I}(T_1 | T_2) = \mathcal{I}(T_1) \parallel \mathcal{I}(T_2)
\]

Each step of the interpretation \( \mathcal{I}_x, \mathcal{I}_u, \mathcal{I}_w \) will be explained in detail in the following subsections.

#### 3.1 Actions to basic actions

A transition from a source state \( s \) when condition \( c \) is satisfied, to a destination state \( t \), with attached general action \( S \), noted as \( s \xrightarrow{c} t \{ S \} \), can be decomposed into a set of intermediate transitions \( U \in \mathcal{U} \), in which the actions in each new transition are basic actions \( B \in \mathcal{B} \).

\[
s \xrightarrow{c} t \{ S \} \xrightarrow{\mathcal{I}_x} U
\]

where \( U \xrightarrow{s_1} s_2 \{ B_1 \} \parallel U_1 \parallel U_2 \), and \( B_i \in \mathcal{B} \).

We use \( \mathcal{I}_x(T) \) to represent this interpretation from a general transition \( T \in \mathcal{T} \) to basic transition \( U \in \mathcal{U} \). The interpretation of the transitions can be parallel.

\[
\mathcal{I}_x(T_1 | T_2) = \mathcal{I}_x(T_1) \parallel \mathcal{I}_x(T_2)
\]

We also use the notation \( \mathcal{I}_x \) to note this transformation, the action \( S \) is decomposed into \( B_1; B_2 \), where \( B \) is the basic actions from the beginning of \( S \), and \( S' \) is the rest.

\[
\mathcal{I}_x(s \xrightarrow{c} t \{ S \}) = \mathcal{I}_x(s, c, t, S', B) \parallel U
\]

where \( U \xrightarrow{S_1} S_2 \parallel B \in \mathcal{B} \) and \( U \in \mathcal{U} \).

- At the very beginning of the interpretation, there is no basic action before \( S \).
- Suppose \( S' = S_1; S_2 \) where \( S_1 \) is the first action of \( S' \). If action \( S_1 \) is a basic action \( S_1 \in \mathcal{B} \), then it can be merged to the previous basic action set \( B \). Otherwise, if \( B \) is empty, decompose \( S_1 \) and \( S_2 \) respectively, and apply the defined rules for each one. If \( B \) is not empty, introduce a new transition for action \( B \), and decompose \( S_1, S_2 \) similarly to the previous case.

The transformation for the composite action \( S \in \mathcal{S} \) and \( S \notin \mathcal{B} \), noted as \( \mathcal{I}_x(S, c, s) = (U, t) \) (where \( s \xrightarrow{c} t \{ S \} \) is the original transition with composite action \( S \), \( U \) is the resulting basic transition), will be represented in the following subsections.

\[
\mathcal{I}_x(S, c, s) = (U, t) \text{ where } S \in \mathcal{S}, \text{ and } S \notin \mathcal{B}, \text{ and } U \in \mathcal{U}
\]

- If there is no action following \( S \) in the interpretation, which means that the action \( S \) is already a basic action \( S \in \mathcal{B} \), then the resulting transition is the same as the original one.

Next, we will interpret each of the composite actions \( S \), \( S \in \mathcal{S} \) and \( S \notin \mathcal{B} \). We write \( \mathcal{I}_x(S, c, s) = (U, t) \) for the action \( S \) from source state \( s \), with guard \( c \). It returns an intermediate transition \( U \) (the actions in \( U \) are the basic actions), and an exit state \( t \).
### 3.1 Condition

A conditional evaluates $S_1$ with the condition $x$ to $U_1$ and $S_2$ with condition not $x$ to $U_2$.

$$I'_T(\text{if } x \text{ then } S_1 \text{ else } S_2, c, s) - \begin{cases} s \xrightarrow{c \text{ and } x} s_1 & U_1 \\ s \xrightarrow{c \text{ and not } x} s_2 & U_2 \end{cases}, u$$

where $I_{TS}(s_1, \text{true}, u, S_1, \phi) = U_1$, $I_{TS}(s_2, \text{true}, u, S_2, \phi) = U_2$

### 3.2 Loops

A loop statement for $(x \in X) \{S\}$ allows iterations over finite integer ranges or over unparameterized enumerated types, which are specified by a data classifier.

#### Integer range

For an integer range, $i \in \mathbb{Z}$, which means that $M$ and $N$ are two integers and $M < N$, the loop statement can be refined as:

$$I'_T(\text{for } i \in M..N \{S\}, c, s) = \begin{cases} s \xrightarrow{U} \{i := M\} \\ u \xrightarrow{v \in N} \{i := i + 1\} \\ v \xrightarrow{w} \end{cases}, w, \text{where } I_{TS}(t, \text{true}, u, S, \phi) = U$$

#### Enumeration range

For an iteration over unparameterized enumeration, $x \in X$, in which $X$ is a data classifier of enumerated type $X = \{x_1, x_2, ..., x_n\}$, the loop statement can be translated as:

$$I'_T(\text{for } x \in X \{S\}, c, s) = \begin{cases} s \xrightarrow{U} \{i := M\} \\ u \xrightarrow{v \in N} \{i := i + 1\} \\ v \xrightarrow{w} \end{cases}, w$$

where $X = \{x_1, x_2, ..., x_n\}$, $|X| = n$, and $I_{TS}(t, \text{true}, u, S, \phi) = U$

### 3.3 Computation

$\text{Computation}(m, n)$ expresses the use of CPU for a possibly non-deterministic period of time between $m$ and $n$.

For this non-deterministic choice, we introduce a function $\text{random}(m, n)$ to choose a random period $r$ ($m < r \leq n$) while translating. In each iteration of $i$, a synchronization with a physical tick $ms$ is performed.

$$I'_T(\text{computation } (m, n), c, s) = \begin{cases} s \xrightarrow{U} t \{i := 1\} \\ u \xrightarrow{v \in N} t \{\text{ms}?!; i := i + 1\} \\ v \xrightarrow{w} \end{cases}, u$$

where $r \sim \text{random}(m, n)$, and $\text{ms}?!$ synchronizes with the physical tick

### 3.4 Delay

The difference between delay and computation is that computation consumes CPU, while delay does not, which means that, when a thread delays some time interval, other threads can execute during this time.

The interpretation of delay is more complicated, for it will request for rescheduling. We can represent the delay using a finite loop if its period can be determined by a random choice:

$$I'_T(\text{delay } (m, n), c, s) - I'_T(\text{for } i \in 1..r \{\text{ms}?!\}, c, s) - (U, t)$$

where $r \sim \text{random}(m, n)$, and $\text{ms}?!$ synchronizes with the physical tick

### 3.2 Basic actions to SSA form actions

Only one new value of a variable $x$ should at most be defined within an instant in SSA form. An operation $x := f(y, z)$ takes the current value of $y$ and $z$ to define the new value of $x$ by the product with $f$. A statement $p(x)$ sends the value $x$ to $p$. Execution may continue within the same symbolic instant unless a second emission is performed. A statement $p(x)$ waits a signal from $p$.

We use the notation $I_U$ to note the intermediate transition $U \in \mathbb{U}$ (with actions $B \in \mathbb{B}$) to be represented in SSA form $W \in \mathbb{W}$ (with actions $A \in \mathbb{A}$).

We use an environment $E$ to associate each variable with its definition, an expression that locates it, $E : X \rightarrow \mathbb{W}$. The environment of $x$ is noted $E(x)$, and the domain of $E$ is noted $\mathcal{V}(E)$. The restriction of a variable $x$ to environment $E$ is noted $E[x]$, which satisfies:

$$\phi[x = \phi]$$

$$(E \cup \{y \mapsto z\})[x] = \begin{cases} E[\phi[x = \phi]] & \text{if } y = x \\
(E[x]) \cup \{y \mapsto z\} & \text{if } y \neq x \end{cases}$$

We write $\text{use}_E(x)$ for the expression that returns the definition of the variable $x$ in environment $E$, and $\text{def}_E(x)$ for the environment $E$ storing variable $x$ with its associated definition.

$$\text{use}_E(x) = \begin{cases} E(x) & \text{if } x \in \mathcal{V}(E) \\
\text{otherwise} & \end{cases}$$

$$\text{def}_E(x) = \{E(x) \cup \{x \mapsto x'\} \mid x' \notin \mathcal{V}(E)$$

We depict sequence of basic actions $B = B_1; B_2$ attached to an intermediate transition $U$ defined in environment $E$ to a set of new SSA form transitions $W$ with an updated environment $F$, in which all the new actions $A$ are in SSA form, and can be executed in the same instant. We use $I_U(U)$ to note this interpretation from an intermediate transition to SSA form transition $W \in \mathbb{W}$, and we introduce another notation $I_U$ to define the transformation rules:

$$I_U(s \xrightarrow{U} t \{B\}) = W \text{where } \begin{cases} I'_U(B_1, B_2, s, E) = (W, t, F) \\
B = B_1; B_2 \end{cases}$$

The following transformations can be defined:

- For a single assignment basic action $a : f(y, z)$ in a transition with environment $E$, the new transition will take its SSA form assignment: the final version of variable $x$ and the definition of $y$ and $z$ defined in $E$ are used, the new environment $F$ only stores the final value of $x$ defined in $E$. 
The send message action can be merged if $p \to p'$ has not been defined in $E$, and $\{ p \mapsto p' \}$ is added to update $E$. Otherwise, create a transition attached with the actions $B_1$ and the final values of all variables $x$ defined in $E$. And apply the transformation rules for the rest of the actions with an environment $\{ p \mapsto p' \}$.

$$I_\mathcal{U}(B_1, (p\langle x \rangle; B_2), s, E) = I_\mathcal{U}((B_1; f(x) := \cdot p), B_2, s, F) \text{ where } F = def_e(x)$$

3.3 SSA to Signal

Finally, all the transitions/actions can be represented in the following form:

$$p \rightarrow t[A] / \mathcal{W}$$

where $t \in def(A), x$ occurs at most once in $A$

$$p \rightarrow t[A] := f(y, z) / A_1; A_2$$

The interpretation $I_A(A)\mathcal{W} = (P, F)$ of an SSA form action $A$ takes as parameters the environment $E$ and the guard $g$ that leads to it. It returns a process $P$, and an updated environment $F$.

$$I_A(x := f(y, z))\mathcal{W} = (x := f(a \text{ when } g, b \text{ when } g), F)$$

where

$$I_A(x := f(y, z))\mathcal{W} = (x := f(a \text{ if } y \in E, \text{ else } y), F)$$

$$I_A(x := f(y, z))\mathcal{W} = (x := f(b \text{ if } z \in E, \text{ else } z), F)$$

$$I_A(x := f(y, z))\mathcal{W} = (x := f(F), F)$$

3.4 A Case study

The intermediate generated code of the basic transitions/actions (step $T \rightarrow U$) for the door_handler thread (previously presented in Figure 1) is depicted in Figure 2. It contains a transformation of the transitions as well as their attached actions. The interpretation introduces two intermediate states: $STATE_0, STATE_1$. The first three transitions rewrite the first original one. A transition is introduced for each branch of the condition action.

Figure 2. Intermediate Behavior code

In this example, the SSA form of transitions is the same as depicted in Figure 2, since all the variables are already uniquely defined in each of the transitions. Each transition will then be interpreted to Signal equations. The generated code for the first SSA form transition is listed here, the guard and state variables $(st, nst)$ are added.
Towards a Formal Semantics

