Index of Semantic Rules ........................................ 33
Index of Calls to Semantic Rules .............................. 35
1. Semantics of modules .......................................................... 18
2. Function Inputs for Module .................................................. 18
3. Cycle for modules .............................................................. 19
4. Module or controller memory ................................................. 19
5. Composition of controllers .................................................. 20
6. Renaming controller ........................................................... 20
7. Semantics of controllers ....................................................... 21
8. Cycle for controllers ........................................................... 22
9. Composition of machines .................................................... 22
10. Renaming machine ............................................................ 22
11. Semantics of state machine .................................................. 23
12. Semantics of state machine .................................................. 23
13. Get and set channels .......................................................... 23
14. Cycle for machines ............................................................ 23
15. Constants Initialisation for State Machines ......................... 24
16. Behaviour of state machine ................................................ 24
17. Semantics of state machine .................................................. 24
18. State-machine memory ....................................................... 25
19. Get and Set channels .......................................................... 25
20. Semantics of defined operations .......................................... 25
21. Node container semantics ................................................... 25
22. Node container behaviour ................................................... 26
23. Semantics of node container ................................................ 26
24. Node container core behaviour ............................................. 26
25. Semantics of Transitions ..................................................... 26
26. Semantics of a Transition .................................................... 27
<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>Transition events</td>
<td>27</td>
</tr>
<tr>
<td>28</td>
<td>Semantics of a transition’s trigger</td>
<td>27</td>
</tr>
<tr>
<td>29</td>
<td>Rename transition trigger events</td>
<td>28</td>
</tr>
<tr>
<td>30</td>
<td>Semantics of SimCall</td>
<td>28</td>
</tr>
<tr>
<td>31</td>
<td>Semantics of OutputCommunication</td>
<td>28</td>
</tr>
<tr>
<td>32</td>
<td>ExecStatement</td>
<td>28</td>
</tr>
</tbody>
</table>
In this report, we present a state-machine based notation, called RoboSim, designed specifically for the modelling of verified simulations for robotic applications. As a graphical notation, RoboSim is intended to be more appealing than programming notations; furthermore, a model in RoboSim should be considered as an intermediate, implementation independent, representation that can be translated into languages used by several well-established simulators such as Netlogo [16], MASON [11], JASON [8], Argos [5], Enky (home.gna.org/enki/), Microsoft Robotics Developer Studio (www.microsoft.com/robotics), Webots, and Simulink + Stateflow [12, 13]. The graphical notation of RoboSim is inspired on RoboChart [9], a UML-like notation designed for robotics. However, as a simulation notation, it has the following:

- A model in RoboSim specifies a cyclic mechanism, as is usual in languages like Netlogo and Stateflow, among others.
- The cycle itself is a separate mechanism from the executing machine; a RoboSim model is formed of the parallel execution of the cycle and the machine.
- Time information is restricted to the cycle; the model of the machine is untimed.
- The visible events are readings and writings in registers of sensors and actuators.
- These events are always available.

Additionally, RoboSim has some distinguishing features.

- The cycle step can be more flexibly defined than, for instance, in Stateflow. Particularly, a step is not constrained to entering a single state of the machine.
- A formal semantics for RoboSim is given in the same framework as that for RoboChart, which allows the definition of a notion of correct simulation with respect to the more abstract...
Chapter 1. Introduction

RoboChart model.

- Other relevant properties of a simulation can also be mechanically checked like. For instance, the improper execution of the same operation more than once in a same cycle.

Like RoboChart, apart from the state-machine itself, RoboSim includes elements to organise specifications, fostering reuse and taming complexity.

The state-machine notation is fully specified, including an action language and constructs to specify timing and properties. Operations used in a state machine can be taken from a domain-specific API or defined by other state machines; communication between state machines is synchronous. Operations can be given pre and postconditions.

In this report, we formalise the semantics of RoboSim using CSP [3]. Importantly, CSP is a front end for a mathematical model that supports a number of analysis techniques that allow, for example, checking the validity of a simulation. For that we can use model-checking, which provides a high degree of automation, as well as more powerful (but not automatic) verification based on theorem proving. Use of CSP enables model checking with FDR [15]. On the other hand, CSP has an underlying model based Hoare and He’s Unifying Theories of Programming [4] that makes our core semantics adequate for theorem proving and for extension to deal, for instance, with probability [6].

The remainder of this manual is structured as follows. Chapter 2 presents the RoboSim metamodel, and Chapter 3 defines their well-formedness conditions. The semantics is presented in Chapter 4. Finally, Chapter 5 concludes with a summary of the results and future work.
2. **RoboSim metamodel**

*RoboSim* models are structured using the elements sketched in Figure 2.1. The structure of a *RoboSim* package follows *RoboChart* structure, namely, modules, robotic platforms, controllers, simulation machines.

A simulation is defined by a Module, which includes a robotic platform and at least one Controller, which can each include one or more simulation machines. In the metamodel, Robotic-Platforms, Controllers, and StateMachines are ConnectionNodes. The restrictions on cardinality are well-formedness conditions. The ConnectionNodes are linked by Connections via their events from and to. The connections can be asynchronous and bidirectional; further restrictions are well-formedness conditions.

Modules, controllers, and machines are self-contained: they declare the full Context (variables, operations, and events) used in their definitions, possibly via interfaces, to allow compositional reasoning. The main difference from *RoboChart* is that these elements include the cycle definition.

A variable cycle of type *nat* of natural numbers is implicitly declared in every model. Its value is defined by a boolean Expression given in each module, controller, and state machine, so that they are self-contained. Modules, controllers, and state machines define the valid sample times for their simulation by specifying restrictions on the value of cycle.

The cycle specifications may admit several valid periods. In general, however, an actual value needs to be defined just in association with a particular simulation execution. If a component (module, controller, or machine) does not explicitly specify it, a value for cycle that satisfies the specification can be identified, for example, when generating code for a simulator.
A module and each of its controllers may have different specifications for the value of \( \text{cycle} \); similarly, a controller and each of its machines may also have different specifications. Ultimately, it is the module that defines the \( \text{cycle} \) of the simulation of a complete model. There has to be, therefore, at least one value that satisfies all the restrictions of the module and its controllers, or of a controller and its state machines.

A simulation-machine definition (SimMachineDef) is a StateMachine. Another form of StateMachine, is a reference to a state machine.

Declarations in a simulation machine are partitioned into three Contexts: local declarations, inputs and outputs. Input and output events have a semantics different from that in RoboChart. There, they are events raised by the platform or the software. In RoboSim, an input or output is represented by a boolean that indicates whether that event has occurred. If any values are communicated, they are meaningful only if the event occurs.

Calls to operations are treated as outputs in RoboSim. Programmatically, in a simulation cycle, operations may be called during the processing of inputs, but are only actually executed later, at the point of the cycle when the registers are written.
A required variable is also external to the machine, and so its value is read, in the case of an input variable, and written, for output variables, on a cyclic basis. A variable or event may be both an input and an output.

To make the semantic differences clear, references to inputs and outputs are all preceded by a $ in RoboSim. In the metamodel (see Figure 2.1), we have an extra form of Expression that allows the use of an input Event as a variable (InputCommunication). If the input communicates a value, that is recorded as part of that communication. An InputCommunication can take place only as part of a transition trigger, so that any variable assignments are an implicit part of the transition assignment. Expressions do not have side effects. Another new form of Expression, namely, RequiredVariable, allows references to a variable preceded by a $.

OutputCommunications and OperationCalls can be used in actions, and are, therefore, extra forms of Statement. Like RoboChart, RoboSim allows other types of Statement such as Assignment, which assigns a value to a variable, IfStmt, which conditionally executes one of two statements, and Clock Reset, which allows to reset a clock. A special form of Transition, namely, SimTransition, allows the use of the special event exec as a trigger; it does not need to be declared. No other triggers are possible in a RoboSim model.

Despite the semantic distinctions, we have interface declarations in RoboSim exactly like in RoboChart, since this facilitates the modularisation of declarations, and the transition from a RoboChart to a RoboSim model. Particularly, this allows the designer to reuse entirely the robotic platform in the simulation.

As opposed to RoboChart clocks, RoboSim clocks advance in each cycle by the number of time units of the period for the cycle. So, choice of that period needs to take into account the budgets and deadlines required for the model.
3. Well-formedness Conditions

We now define a number of well-formedness conditions that identify the valid models written using the RoboSim metamodel presented in the previous chapter. Many conditions are those expected of a standard state-machine notation, and are fully described in the definition of RoboChart [9]. In what follows, we present the well-formedness conditions that are specific to RoboSim or related to constructs specific to RoboSim.

3.1 Robotic Platforms

The well-formedness conditions associated with robotic platforms involve the declaration of elements of the provided interfaces.

SRP1 Provided interfaces must declare just variables and operations. There is no notion of providing events in RoboSim, since events are taken to be elements of a component, which are used to establish a connection with another component for communication.

3.2 Modules

SM1 The specification of $\text{Cycle}$ is a boolean expression. It is a predicate that specifies a restriction on the values (positive natural numbers) that the variable $\text{Cycle}$ may take.

SM2 The conjunction of the $\text{Cycle}$ specification of all the controllers and of the module itself is not false. This means that it is possible to choose a valid positive value for $\text{Cycle}$ for use in a simulation of the module.
Chapter 3. Well-formedness Conditions

SM3 The outputs of the controllers are disjoint, so that there is no conflict when writing to the actuator registers. In the case of events, this is ensured by the connections like in RoboChart: an event of the platform is linked to at most one controller. Required variables, however, may be required by several controllers, and should be an output just in one. An operation should be required just by one controller.

SM4 The RoboChart facility for creating module instances (related to collections) is not allowed.

3.3 Controllers

SC1 The specification of cycle is a boolean expression.

SC2 The conjunction of the cycle specifications of all the simulation machines, of all the machines that define operations, and of the controller itself is not false. Besides machines, a controller may define operations used by its machines. These operations may be defined by simulation machines themselves, and their cycle specifications also need to be feasible in the context of the controller. This condition is similar to SM2, but refers to the specifications of cycle in the machines of a controller and in the controller itself, while SM2 refers to the specifications of the controllers of a module and of the module itself. SM2 is not concerned with restrictions in machines.

SC3 Connections with a simulation machine must respect its input and output definitions. For instance, an input event of a machine must be either not connected or the connection must be an input to that machine. Similarly for outputs: they must be either not connected, or connected to an output from that machine.

SC4 The outputs of the state machines are disjoint, to avoid conflicts as in the case of module.

3.4 State Machine

SSTM1 The specification of cycle is a boolean expression.

SSTM2 Input declarations can be only events and variables.

SSTM3 Output declarations can be events, variables, or operations.

SSTM4 Required variables must be inputs and outputs, since they can be read and written, like in RoboChart.

SSTM5 Variables defined in a machine are there only for local use.

SSTM6 All platform operations must be outputs. Calls to operations provided by the controller, however, do not become outputs of the system.

SSTM7 Inputs, outputs, and required variables are referenced using a $. This emphasises the fact that they are handled in a cyclic pattern.

SSTM8 Local event declarations are not allowed.

SSTM9 The input and output contexts have only events and interfaces that can be defined or required.
3.5 Transitions

**ST1** A transition cannot have deadline and probability junctions.

**ST2** The only possible trigger is exec.

3.6 Statements

**SS1** Timed and wait statements are not allowed.

3.7 Events

**SE1** There is no broadcast attribute.

**SE2** Exec is the only possible event that can be used as trigger.
The semantics of RoboSim is based on the timed semantics of RoboChart, which is fully described in the RoboChart reference manual [9]. In what follows, we present the rules that are specific to RoboSim.
Rule 1. Semantics of modules

\[ \begin{align*}
[m : SimModule], M : \text{TimedCSPProcess} = \\
\left\{ \begin{array}{l}
cycleModule^1(m, \text{ctrls}, \text{inputs}, \text{outputs}, \text{rvars}, \text{evars}) \\
\{ \{\text{registerWriteC}, \text{data}(v) \mid v : \text{ran}\text{rvars}\} \cup \{\text{registerWriteE}\}\} \\
\text{memoryComp}^1(\text{rvars}, \text{evars}, \text{rp}) \\
\{\{\text{registerWriteE}\}\} \\
\{\text{setConstants}\} \\
\{\{\text{registerReadC}, \text{registerWriteC}, \text{endExecC}, \text{end}\}\} \\
\{\text{composeControllers}\} \\
\{\{\text{end}\}\} \text{ SKIP}
\end{array} \right.
\end{align*} \]

where

\begin{align*}
\text{rp} &= \text{roboticPlatformDefinition}(m) \\
\text{ctrls} &= \text{controllersDefinition}(m) \\
\text{cons} &= m.\text{connections} \\
\text{inputs} &= \text{Inputs}(\text{rp}, \text{cons}) \\
\text{outputs} &= \text{Outputs}(\text{rp}, \text{ctrls}) \\
\text{rvars} &= Rvars(\text{rp}, \text{ctrls}) \\
\text{evars} &= \text{Internals}(\text{cons}) \\
\text{setConstants} &= \{c : \text{allConstants}(\text{rp}) \text{ * set name}(c)\} \\
\text{endExecC} &= \{c : \text{ctrls} \text{ * endexec.} \text{id}(c)\}
\end{align*}

Rule 2. Function Inputs for Module

\begin{align*}
\text{Inputs}(\text{rp} : \text{RoboticPlatform}, \text{cons} : \text{Set(Connection)}) : \text{Set(InputsType)} = \\
\{\{c : \text{cons} | c.\text{from} = \text{rp} \land c.\text{to} \in \text{Controller} \text{ * (id(c.efrom), id(c.eto))}\}\}
\end{align*}
4.1 Module 19

**Rule 3. Cycle for modules**

cycleModule(m : SimModule, ctrls : Seq(SimControllerDef), inputs : Set(InputsType), 
outputs : Set(OutputsType), rvars : Set(OutputsType), evars : Set(EventsType)) : TimedCSPProcess =

let CycleModule =

\[
\begin{align*}
&\{\begin{array}{l}
(\| in : dom inputs \rightarrow registerReadC.take(in) \rightarrow registerReadC.give(inputs(in)) \rightarrow SKIP); \\
(\| evar : dom evars \rightarrow registerReadC.take(evar) \rightarrow SKIP); \\
(\| evar : dom evars \rightarrow registerWriteE.data(evar) \rightarrow SKIP); \\
(CollectOutputs(dom(outputs)) \{ endexec.id(m) \} \ Monitor) \ \triangle Stop; \\
\end{array}\} \rightarrow (end \rightarrow SKIP)^> (wait(\{m.cycleDef[\text{Expr} - 1]\}); \\
\} CycleModule;
\end{align*}
\]

CollectOutputs(sout) =

\[
\begin{align*}
&\{\begin{array}{l}
\text{CollectOutputs(sout)} = \text{CollectOutputs(sout)} \cup \{\text{CollectOutputs(sout)} \setminus \{\text{CollectOutputs(sout)}\}\text{project(output)}\} \\
\end{array}\} \rightarrow \text{CollectOutputs(sout)} \setminus \{\text{CollectOutputs(sout)}\}\text{project(output)}); \\
\end{align*}
\]

Monitor =

\[
\begin{align*}
&\{\begin{array}{l}
\text{Monitor} = \text{CollectOutputs(sout)} \cup \{\text{CollectOutputs(sout)} \setminus \{\text{CollectOutputs(sout)}\}\text{project(output)}\); \\
\end{array}\} \rightarrow \text{CollectOutputs(sout)} \setminus \{\text{CollectOutputs(sout)}\}\text{project(output)}; \\
\end{align*}
\]

The function \text{take} maps an input or output to CSP input parameters of a communication.

**Rule 4. Module or controller memory**

memoryComp(rvars : Set(OutputsType), evars : Set(EventsType), node : ConnectionNode) : TimedCSPProcess =

let Memory(nvars) =

\[
\begin{align*}
&\{\begin{array}{l}
\text{Memory}(nvars) = \text{Memory}(nvars) \cup \{\text{Memory}(nvars)\}; \\
\text{registerWriteC.take(v) \rightarrow Memory(nvars[\text{name}(v) := true]);} \\
\text{registerWriteE.take(v) \rightarrow Memory(nvars[\text{name}(v) := false]);} \\
\text{registerWriteC.take(v) \rightarrow Memory(nvars);} \\
\text{registerReadC.give(rvars) \rightarrow Memory(nvars);} \\
\text{registerReadC.give(rvars) \rightarrow Memory(nvars);} \\
\end{array}\} \rightarrow \text{Memory}(nvars); \\
\}
\end{align*}
\]

The function \text{composeControllers}\(^2(m, ctrls, inputs, outputs, rvars, evars)\) basically constructs a parallelism of the processes for each of the controllers in the sequence \text{ctrls}.
**Rule 5. Composition of controllers**

\[
\text{composeControllers}(m : \text{SimModule}, \text{ctrls} : \text{Seq}(\text{SimControllerDef}), \text{inputs} : \text{Set}(\text{InputsType}), \text{outputs} : \text{Set}(\text{OutputsType}), \text{rvars} : \text{Set}(\text{OutputsType}), \text{evars} : \text{Set}(\text{EventsType}) : \text{TimedCSPProcess} =
\]

\[
\text{if } \#\text{ctrls} = 1 \text{ then}
\]

\[
\text{renamingController}^1(m, \text{headctrls}, \text{inputs}, \text{outputs}, \text{rvars}, \text{evars})
\]

\[
\text{else}
\]

\[
\text{renamingController}^2(m, \text{headctrls}, \text{inputs}, \text{outputs}, \text{rvars}, \text{evars})
\]

\[
\{\{\text{end}\} \cup \text{setConstants}\}
\]

\[
\text{composeControllers}^3(m, \text{tailctrls}, \text{inputs}, \text{outputs}, \text{rvars}, \text{evars})
\]

\[
\text{where}
\]

\[
\text{setConstants} = \{c : \text{allConstants}(rp) \times \text{set}_\text{vid}(c, m)\}
\]

**Rule 6. Renaming controller**

\[
\text{renamingController}(m : \text{SimModule}, c : \text{SimControllerDef}, \text{inputs} : \text{Set}(\text{InputsType}), \text{outputs} : \text{Set}(\text{OutputsType}), \text{rvars} : \text{Set}(\text{OutputsType}), \text{evars} : \text{Set}(\text{EventsType}) : \text{TimedCSPProcess} =
\]

\[
\llbracket c \rrbracket
\]

\[
\begin{align*}
\{\text{ct} : \text{allConstants}(c) \times \text{set}_\text{vid}(\text{ct}) & \leftarrow \text{set}_\text{vid}(\text{ct}, m)\} \\
\bigcup \{\text{registerRead} & \leftarrow \text{registerRead}_C\} \\
\bigcup \{\text{registerWrite} & \leftarrow \text{registerWrite}_C\}
\end{align*}
\]

\[
\setminus \text{setNotConnectedEvs}
\]

\[
\text{where}
\]

\[
\text{setNotConnectedEvs} = \{\{\text{NotConnectedEvs}(\text{inputs}, \text{outputs}, \text{rvars}, \text{evars})\}\}
\]
Rule 7. Semantics of controllers

\[
\begin{align*}
\text{let} & \quad \text{for each } \op : \text{c.lOperations} \cdot \\
& \quad \text{nproc}(\op)(\{x : \op.\text{parameters} \cdot x.\text{name}\}) = [\text{opdef}(\op)]^{\text{nops}}_{\text{STM}} \\
\text{within} & \quad \left(\begin{array}{l}
\text{cycleController}(\{c, \text{inputs, outputs, dvars, evars}\} \\
\text{memoryComp}(\{dvars, evars, c\}) \\
\text{composeMachines}(\{\text{machines, inputs, outputs, dvars, evars}\}^{\text{nops}}_{\text{STM}}) \\
\end{array}\right) \\
\Theta_{\text{end}} & \quad \text{SKIP}
\end{align*}
\]

where

\[
\begin{align*}
\text{machines} & = (x : \text{c.machines}) \\
\text{cons} & = \text{c.connections} \\
\text{inputs} & = \text{InputsC}(c, \text{cons}) \\
\text{outputs} & = \text{OutputsC}(c, \text{cons}) \\
\text{dvars} & = \text{DvarsC}(c) \\
\text{evars} & = \text{InternalsC}(c, \text{cons}) \\
\text{setConstants} & = \{\text{ct : allConstants(c) \* \text{set_name(ct)}\} \\
\text{endExecM} & = \{\text{stm : machines \* \text{endexec}.id(stm)}\} \\
\text{opdef}(\op) & = \text{findOperationDefinition}(\op, \text{c.lOperations}) \\
\text{nops} & = \{\text{op : c.lOperations \* \text{id}(op) \rightarrow \text{nproc}(op)}\} \\
\text{lvars} & = \{v : \text{allLocalVariables(c) \* \text{set_vid(v)}}\} \\
\text{rvars} & = \{v : \text{requiredVariables(c) \* \text{set_Extvid(v)}}\} \\
\text{lconsts} & = \{v : \text{allLocalConstants(c) \* \text{set_vid(v)}}\} \\
\text{rconsts} & = \{v : \text{requiredConstants(c) \* \text{set_vid(v)}}\}
\end{align*}
\]
Chapter 4. Semantics

**Rule 8. Cycle for controllers**

\[
\text{cycleController(c : SimControllerDef, inputs : Set(EventsType), outputs : Set(OutputsType), dvars : Set(OutputsType), evars : Set(EventsType)) : TimedCSPProcess} = \\
\text{let } \text{CycleController} = \\
\begin{array}{l}
\text{if } \# \text{machines} = 1 \\
\text{then } \text{renamingMachine}^1 (c, \text{headmachines, inputs, outputs, rvars, evars}) \\
\text{else } \text{renamingMachine}^2 (c, \text{headmachines, inputs, outputs, rvars, evars}) \\
\end{array}
\]

**Rule 9. Composition of machines**

\[
\text{composeMachines(c : SimControllerDef, machines : Seq(SimMachineDef), inputs : Set(EventsType), outputs : Set(OutputsType), rvars : Set(OutputsType), evars : Set(EventsType)) : TimedCSPProcess} = \\
\text{if } \# \text{machines} = 1 \\
\text{then } \text{renamingMachine}^1 (c, \text{headmachines, inputs, outputs, rvars, evars}) \\
\text{else } \text{renamingMachine}^2 (c, \text{headmachines, inputs, outputs, rvars, evars}) \\
\text{composeMachines}^2 (c, \text{tailmachines, inputs, outputs, rvars, evars}) \\
\text{where} \text{setConstants} = \{ \text{stm : run machines, c : allConstants(stm) • set_vld(c)} \}
\]

**Rule 10. Renaming machine**

\[
\text{renamingMachine(c : SimControllerDef, stm : SimMachineDef, inputs : Set(EventsType), outputs : Set(OutputsType), rvars : Set(OutputsType), evars : Set(EventsType)) : TimedCSPProcess} = \\
\begin{array}{l}
\text{if } \# \text{machines} = 1 \\
\text{then } \text{renamingMachine}^1 (c, \text{headmachines, inputs, outputs, rvars, evars}) \\
\text{else } \text{renamingMachine}^2 (c, \text{headmachines, inputs, outputs, rvars, evars}) \\
\end{array}
\]

\[
\text{setNotConnectedEvs = } \{ \text{NotConnectedEvs(inputs, outputs, rvars, evars)} \}
\]
4.3 State Machines

**Rule 11. Semantics of state machine**

\[ \text{stm} : \text{StateMachineBody} \]

\[ \text{STM} : \text{TimedCSPProcess} = \]

The rule is split according to the type of \text{stm}.

**Rule 12. Semantics of state machine**

\[ \text{stm} : \text{SimMachineDef} \]

\[ \text{STM} : \text{TimedCSPProcess} = \]

\[
\begin{align*}
\text{behaviour}^1(\text{stm}) & \left\langle \text{getsetChannelsStm}^1(\text{stm}) \cup \{\text{registerWrite}\} \right\rangle \setminus \text{getsetChannelsStm}^2(\text{stm}) \\
\text{stmMemory}^1(\text{stm}) & \left\langle \{\text{startexec}, \text{endexec}, \text{id}(\text{stm}), \text{end}, \text{registerRead}, \text{registerWrite}\} \right\rangle \\
\text{cycle}^1(\text{stm}, \text{inputs}, \text{outputs}) & \left\langle \{\text{startexec}\} \right\rangle
\end{align*}
\]

\[ \Theta_{\text{(end)}} \text{SKIP} \]

where

\[ \text{inputs} = \text{inputs}(\text{stm}) \]
\[ \text{outputs} = \text{outputs}(\text{stm}) \]
\[ \text{reqVars} = \text{reqVars}(\text{stm}) \]
\[ \text{consts} = \text{allConstants}(\text{stm}) \]

**Rule 13. Get and set channels**

\[ \text{getsetChannels}(\text{stm} : \text{SimMachineDef}) : \text{ChannelSet} = \]

\[ \left\langle \{v : \text{Evars}(\text{stm}) \cdot \text{get}_{\text{vlid}}(v)\} \cup \{v : \text{Rvars}(\text{stm}) \cdot \text{get}_{\text{vlid}}(v)\} \cup \right\rangle \]

\[ \left\langle \{v : \text{allConstants}(\text{stm}) \cdot \text{get}_{\text{vlid}}(v)\} \cup \{v : \text{allLocalConstants}(\text{stm}) \cdot \text{set}_{\text{vlid}}(v)\} \right\rangle \]

**Rule 14. Cycle for machines**

\[ \text{cycle}(\text{stm} : \text{SimMachineDef}, \text{inputs} : \text{Set}(<\text{InputType}>), \text{outputs} : \text{Set}(<\text{OutputType}>)) : \]

\[ \text{TimedCSPProcess} = \]

let \( \text{Cycle} = \)

\[
\begin{align*}
\left(\left(\left(\left(\left(\text{in} \cdot \text{registerRead}.\text{take}(\text{in}) \rightarrow \text{SKIP}\right)\right)\rightarrow \text{CollectOutputs}(\text{outputs})\right)\rightarrow \text{Stop}^1\right) ; \\
\text{startexec} \rightarrow \text{CollectOutputs}(\text{outputs}) \rightarrow \text{Start}^1\right) ; \\
\left(\left(\text{end} \rightarrow \text{SKIP}\right) \rightarrow_1 \text{wait}(\left[\text{stm.cycleDef} \cup \text{expr} - 1\right])\right) ; \\
\text{Cycle} \rightarrow \text{CollectOutputs}(\text{sout}) = \text{registerWrite}\cdot\text{give}(\text{sout}) \rightarrow \text{CollectOutputs}(\text{sout}\ \cup \{\text{sout}\}) \\
\rightarrow_1 \text{endexec}.\text{id}(\text{stm}) \rightarrow \text{SKIP}
\end{align*}
\]

within \( \text{Cycle} \)
Rule 15. Constants Initialisation for State Machines

\[
\text{constInitSTM}(cs : \text{Seq}_1(\text{Variable}), \text{stm} : \text{StateMachineDef}, P : \text{CSPProcess}) : \text{TimedCSPProcess} = \\
\text{buildScope}(\text{undefc}, \text{stm}, \left( \begin{array}{l}
\text{let } c : \text{def} \cdot \text{name}(c) = \llbracket c.\text{initial} \rrbracket \text{Expr} \\
\text{within}_P
\end{array} \right))
\]

where
\[
\text{defc} = (x : \text{consts} | x.\text{initial} \neq \text{null}) \\
\text{undefc} = (x \cdot \text{consts} | x.\text{initial} = \text{null})
\]

Rule 16. Behaviour of state machine

\[
\text{behaviour}(\text{stm} : \text{SimMachineDef}) : \text{TimedCSPProcess} = \\
\text{let} \\
\text{Ending} = \text{endexec} \rightarrow (\text{startexec} \rightarrow \text{Ending} \sqcap \text{end} \rightarrow \text{SKIP}) \\
\text{within} \\
\left( \begin{array}{l}
(\text{startexec} \rightarrow \text{stateful}(\text{stm}) \setminus \{\text{end}\}) \\
\text{skip} \setminus \text{Ending}
\end{array} \right)
\]

Rule 17. Semantics of state machine

\[
\text{stateful}(\text{stm} : \text{StateMachineBody})^{\text{nops}} : \text{TimedCSPProcess} = \\
\text{let} \\
\text{Stateful} = \\
\text{MachineBody} \\
\left( \begin{array}{l}
\llbracket \text{getsetLocalChannels(} \text{stm}\rrbracket \cup \text{clockSync} \cup \{\text{end}\} \\
\llbracket \text{varMemory(} \text{stm}\rrbracket \llbracket \{\text{end}\} \rrbracket \cup \text{constMemory(} \text{stm}\rrbracket) \\
\llbracket \text{clockstimed(} \text{stm}\cdot\text{clocks}\rrbracket
\end{array} \right)
\]

\text{within} \\
\text{Stateful}

\text{where} \\
\text{clockSync} = \{c : \text{stm}\cdot\text{clocks} \cdot \text{get}_{\text{id}}(c), \text{clockReset}_{\text{id}}(c)\} \\
\text{enteredSS} = \{x : \text{stm}\cdot\text{nodes} \cdot \text{entered}_{\text{id}}(x)\}
4.4 NodeContainers

The semantics of a node container is split into three rules for convenience.

**Rule 21. Node container semantics**

\[
\text{ncBehaviour}^{(\text{nops})} (\text{nc})^{\text{nops}} : \text{TimedCSPProcess} =
\]
**Rule 22.** Node container behaviour

\[
\text{ncBehaviour}(\text{nc} : \text{NodeContainer})^{\text{ops}} : \text{TimedCSPProcess} =
\]
\[
\left(\text{ncCoreBehaviour}^{1}(\text{nc})^{\text{ops}} \setminus \{\text{enter, exit, exited, internal}\}\right) \parallel \text{renameTriggerEvents}^{1}(\text{nc})
\]

**Rule 23.** Semantics of node container

\[
\text{[nc : NodeContainer]}^{\text{ops}} : \text{TimedCSPProcess} =
\]
\[
\left(\text{ncBehaviour}^{2}(\text{nc})^{\text{ops}} \parallel \text{vars}(\text{nc}.\text{nodes}) \parallel \text{flowevts} \parallel \text{transSync}(\text{nc}) \parallel \{\text{end}\} \parallel \{\text{startexec, endexec}\} \parallel \text{vguards}(\text{nc}) : \emptyset\right)
\]

where
\[
\begin{align*}
\text{stateClocks}(\text{nc}) &= \{s : \text{nc}.\text{nodes} | s \in \text{State} \land s \neq \text{Final}\} \\
\text{stateClockSync}(\text{nc}) &= \{n : \text{stateClocks}(\text{nc}) \cdot \text{entered}.\text{id}(n), \text{get}_\cdot\text{id}(n)\}
\end{align*}
\]

**Rule 24.** Node container core behaviour

\[
\text{ncCoreBehaviour}(\text{nc} : \text{NodeContainer})^{\text{ops}} : \text{TimedCSPProcess} =
\]
\[
\left(\text{composeTimedNodes}(\text{nc})^{\text{ops}} \parallel \text{tidsR}(\text{nc}) \parallel \text{vars}(\text{nc}.\text{nodes}) \parallel \text{flowevts} \parallel \text{transSync}(\text{nc}) \parallel \{\text{end}\} \parallel \text{vguards}(\text{nc}) : \emptyset\right)
\]

where
\[
\begin{align*}
\text{tidsR}(\text{nc}) &= \{t : \text{nc}.\text{transitions} \cdot \text{interrupt}.\text{id}(t.\text{src}) \leftarrow \text{tevent}^{1}(t)\} \\
\text{flowevts} &= \{\text{enter, exit, exited, interrupt}\} \\
\text{transSync}(\text{nc}) &= \{t : \text{nc}.\text{transitions} \cdot \text{tevent}^{0}(t)\} \\
\text{vguards}(\text{nc}) &= \{t : \text{nc}.\text{transitions} | \exists v : v \in \text{usedVariables}(t.\text{condition}) \cdot v\}
\end{align*}
\]

### 4.5 Transitions

**Rule 25.** Semantics of Transitions

\[
\text{transitions}(\text{nc} : \text{NodeContainer})^{\text{ops}} : \text{TimedCSPProcess} =
\]

let
\[
\begin{align*}
\text{Trans} &\triangleq \text{readStateA} \\
&\quad \left(\text{vguards}, \begin{align*}
\left(\begin{align*}
\text{share} &\rightarrow \text{Skip} \\
\text{endexec} &\rightarrow \text{startexec} \rightarrow \text{SKIP}
\end{align*}\right) ; \text{Trans}
\end{align*}\right)
\end{align*}
\]

within
\[
\text{Trans}
\]

where
\[
\text{vguards} = \{t : \text{nc}.\text{transitions}, v : \text{NamedElement} | v \in \text{usedVariables}(t.\text{condition}) \cdot v\}
\]
Rule 26. Semantics of a Transition

\[
[t : \text{Transition}]^{\text{nops}}_{\text{TimedCSPProcess}} = \\
\begin{aligned}
&\text{if } \text{src} \in \text{State} \land t.\text{condition} \neq \text{null} \\
&\quad \left( (t.\text{condition})_{\text{Expr}} \& \text{trigger}(t); \text{clockReset(t)}; (SS Stop \triangle \text{exit} \rightarrow \text{Skip}); \right) \\
&\quad ((SS Stop \mid (\mu X \bullet \text{exec} \rightarrow \text{startexec} \rightarrow X)) \triangle \\
&\quad (\text{executed} \rightarrow [t.\text{action}]^{\text{nops}}_{\text{StatementInContext}} [\text{endexec} \leftarrow \text{endexec}\_\text{action}, \text{startexec} \leftarrow \text{startexec}\_\text{action}]); \\
&\quad \text{enter} . \text{id}(\text{tgt}) \rightarrow \text{Skip} \\
&\text{else if } \text{src} \in \text{State} \land t.\text{condition} = \text{null} \\
&\quad \left( \text{trigger}^2(t); \text{clockReset(t)}; (SS Stop \triangle \text{exit} \rightarrow \text{Skip}); \right) \\
&\quad ((SS Stop \mid (\mu X \bullet \text{exec} \rightarrow \text{startexec} \rightarrow X)) \triangle \\
&\quad (\text{executed} \rightarrow [t.\text{action}]^{\text{nops}}_{\text{StatementInContext}} [\text{endexec} \leftarrow \text{endexec}\_\text{action}, \text{startexec} \leftarrow \text{startexec}\_\text{action}]); \\
&\quad \text{enter} . \text{id}(\text{tgt}) \rightarrow \text{Skip} \\
&\text{else if } \text{src} \notin \text{State} \land t.\text{condition} \neq \text{null} \\
&\quad ([t.\text{condition}]_{\text{Expr}} \& \text{internal} . \text{id} (\text{src}) \rightarrow \\
&\quad [t.\text{action}]^{\text{nops}}_{\text{StatementInContext}} [\text{endexec} \leftarrow \text{endexec}\_\text{action}, \text{startexec} \leftarrow \text{startexec}\_\text{action}]); \\
&\quad \text{enter} . \text{id}(\text{tgt}) \rightarrow \text{Skip} \\
&\text{else if } \text{src} \notin \text{State} \land t.\text{condition} = \text{null} \\
&\quad \text{internal} . \text{id} (\text{src}) \rightarrow \\
&\quad [t.\text{action}]^{\text{nops}}_{\text{StatementInContext}} [\text{endexec} \leftarrow \text{endexec}\_\text{action}, \text{startexec} \leftarrow \text{startexec}\_\text{action}]; \\
&\quad \text{enter} . \text{id}(\text{tgt}) \rightarrow \text{Skip} \\
\end{aligned}
\]

where

\[
\text{src} = t.\text{source} \\
\text{tgt} = t.\text{target}
\]
Rule 29. Rename transition trigger events

\[
\text{renameTriggerEvents}(\text{nc : NodeContainer}) : \text{RenamingSet} = \\
\{ t : ts • endexec • \text{id}(t.source) \leftarrow \text{endexec} \} \\
\cup \{ \text{endexec} \_\text{action} \leftarrow \text{endexec} \} \\
\cup \{ \text{startexec} \_\text{action} \leftarrow \text{startexec} \} \\
\text{where} \\
\hspace{1em} ts = \{ t : \text{nc.transitions} \mid t.\text{trigger} \neq \text{null} \}
\]

4.6 Statements

Rule 30. Semantics of SimCall

\[
[\text{stmt : SimCall}]^{\text{nops}}_{\text{Stmt}} : \text{TimedCSPProcess} = \\
\text{if stmt.args \neq \text{null}} \\
\hspace{1em} \text{registerWrite}.\text{stmt.operation.name}!\{ x : \text{stmt.args} • x.\text{name} \} \rightarrow \text{Skip} \\
\text{else} \\
\hspace{1em} \text{registerWrite}.\text{stmt.operation.name} \rightarrow \text{Skip}
\]

Rule 31. Semantics of OutputCommunication

\[
[\text{stmt : OutputCommunication}]^{\text{nops}}_{\text{Stmt}} : \text{TimedCSPProcess} = \\
\text{if stmt.value \neq \text{null}} \\
\hspace{1em} \text{registerWrite}.\text{stmt.event.name}!\{ \text{stmt.value} \}_{\text{expr}} \rightarrow \text{Skip} \\
\text{else} \\
\hspace{1em} \text{registerWrite}.\text{stmt.event.name} \rightarrow \text{Skip}
\]

Rule 32. ExecStatement

\[
[\text{stmt : ExecStatement}]^{\text{nops}}_{\text{Stmt}} : \text{TimedCSPProcess} = \\
\hspace{1em} \text{endexec} \rightarrow \text{startexec} \rightarrow \text{SKIP}
\]
We have presented here, *RoboSim*, a new notation for simulation of robots. We have described a semantics for its core constructs. It uses CSP, but we envisage its extension to use Circus [1], a process algebra that combines Z [7] and CSP, and includes time constructs [2]. Use of Circus and its UTP foundation will enable use of theorem proving as well as model checking. Work on probability is available in the UTP [6], but we will pursue an encoding of Markov decision processes in the UTP.

*RoboChart* itself misses support for modelling the environment and the robotic platforms in model detail. It is also in our plans to take inspiration from hybrid automata [14] to extend the notation, and from the UTP model of continuous variables [10] to define the semantics.


Chapter 5. Conclusions


In this index you’ll find the list of semantic functions in alphabetic order, and page where they are defined.

<table>
<thead>
<tr>
<th>Function</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>stateful (StateMachineBody)</td>
<td>24</td>
</tr>
<tr>
<td>behaviour</td>
<td>24</td>
</tr>
<tr>
<td>C (Controller)</td>
<td>21</td>
</tr>
<tr>
<td>composeControllers</td>
<td>20</td>
</tr>
<tr>
<td>composeMachines</td>
<td>22</td>
</tr>
<tr>
<td>constInitSTM</td>
<td>24</td>
</tr>
<tr>
<td>cycle</td>
<td>23</td>
</tr>
<tr>
<td>cycleController</td>
<td>22</td>
</tr>
<tr>
<td>cycleModule</td>
<td>19</td>
</tr>
<tr>
<td>getsetChannels</td>
<td>25</td>
</tr>
<tr>
<td>getsetChannelsStm</td>
<td>23</td>
</tr>
<tr>
<td>inputs</td>
<td>18</td>
</tr>
<tr>
<td>M (SimModule)</td>
<td>18</td>
</tr>
<tr>
<td>memoryComp</td>
<td>19</td>
</tr>
<tr>
<td>NC</td>
<td>25</td>
</tr>
<tr>
<td>NC (NodeContainer)(Timed)</td>
<td>26</td>
</tr>
<tr>
<td>ncBehaviour</td>
<td>26, 26</td>
</tr>
<tr>
<td>renameTriggerEvents</td>
<td>28</td>
</tr>
<tr>
<td>renamingController</td>
<td>20</td>
</tr>
<tr>
<td>renamingMachine</td>
<td>22</td>
</tr>
<tr>
<td>SimMachineDef</td>
<td>23</td>
</tr>
<tr>
<td>Statement</td>
<td>28, 28</td>
</tr>
<tr>
<td>statement</td>
<td>28</td>
</tr>
<tr>
<td>STM (SimOperationDef)</td>
<td>25</td>
</tr>
<tr>
<td>STM (SState Machine)</td>
<td>23</td>
</tr>
<tr>
<td>stmMemory</td>
<td>25</td>
</tr>
<tr>
<td>T (Transition)</td>
<td>27</td>
</tr>
<tr>
<td>tevent(Transition)</td>
<td>27</td>
</tr>
<tr>
<td>Transitions</td>
<td>26</td>
</tr>
<tr>
<td>triggerForMemory</td>
<td>27</td>
</tr>
</tbody>
</table>
Index of Calls to Semantic Rules

In this index you’ll find the location of call to the semantic rules. For each call of a semantic function, the page number superscripted with the usage index is provided. The index of the call is unique with respect to the semantic function, and also shown superscripted in the call location.

behaviour , 23\textsuperscript{1}
C (Controller) , 20\textsuperscript{1}
composeControllers , 18\textsuperscript{1}, 19\textsuperscript{2}, 20\textsuperscript{3}
composeMachines , 21\textsuperscript{1}, 22\textsuperscript{2}
cycle , 23\textsuperscript{1}
cycleController , 21\textsuperscript{1}
cycleModule , 18\textsuperscript{1}
getsetChannelsStm , 23\textsuperscript{1}, 23\textsuperscript{2}
memoryComp , 18\textsuperscript{1}, 21\textsuperscript{2}
NC , 24\textsuperscript{1}
ncBehaviour , 25\textsuperscript{1}, 26\textsuperscript{2}
ncCoreBehaviour , 26\textsuperscript{1}
renameTriggerEvents , 26\textsuperscript{1}
renamingController , 20\textsuperscript{1}, 20\textsuperscript{2}
renamingMachine , 22\textsuperscript{1}, 22\textsuperscript{2}
stateful , 24\textsuperscript{1}, 25\textsuperscript{2}
STM (State machine) , 21\textsuperscript{1}, 22\textsuperscript{2}
stmMemory , 23\textsuperscript{1}
T (Transition) , 26\textsuperscript{1}
tevent , 26\textsuperscript{1}, 26\textsuperscript{2}
transitions , 26\textsuperscript{1}
trigger , 27\textsuperscript{1}, 27\textsuperscript{2}