## SCXML semantics

The SCXML semantics are described operationally here:-

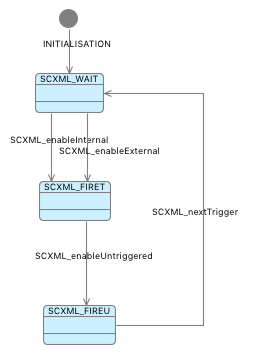
Our (abstract) interpretation is as follows

1. Initialise
2. Take one event from the internal queue and fire the set of transitions that are enabled by it at that time. I.e. they must be enabled at the time it checks, not subsequently after firing one or more of the set of transitions.
3. Fire the set of un-triggered transitions that are enabled after step 1). Again they must be enabled at the time it checks, not subsequently.
4. If the internal queue is not empty, repeat from 1)
5. If the internal queue is empty, and the external queue is empty, wait for an external event to arrive.
6. If the external queue is not empty, take one event from the external queue and fire the set of transitions that are enabled by it at that time. Again they must be enabled at the time it checks, not subsequently after firing one or more of the set of transitions.
7. repeat from 1)

There are some issues with this interpretation

1. The system cannot start because initially the internal queue will be empty.
2. The system cannot progress through a sequence of un-triggered transitions unless irrelevant external/internal triggers arrive. Therefore it is invalid to have more than one un-triggered transition without a triggered one in between.
3. Irrelevant triggers make the system progress through un-triggered transitions.

## SCXML engine

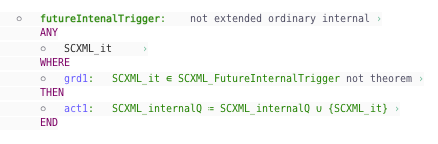
A *basis* machine and context are provided to define the generic elements of the SCXML engine. Specific translated SCXML models start by refining/extending this basis. The basis provides a cyclic engine representing an abstraction of the semantics of SCXML. There are two trigger queues; internal and external. (Currently these are modelled as sets. It would be more accurate to make them queues).

Initially the engine waits for triggers. When a trigger is present, internal triggers have precedence over external ones. A trigger is consumed and used to evaluate the enabledness of the transitions according to the current state of the SCXML application state chart and any other conditions involving system data. A Boolean flag is constructed for each transition recording its enabledness. This flag is used as the guard for the Event-B event that represents the corresponding SCXML transition. The engine then waits for all the transitions it enabled to fire. The transitions set new state and data as well as resetting their enabled flag. They may also raise new internal triggers by adding them to the internal queue.

When all flags are reset to FALSE, the engine evaluates the enabledness of the transitions that are not triggered. This is done in a similar way using Boolean flags. When all un-triggered transitions have fired the engine goes back to the start and consumes another trigger from the internal queue if there is one, or from the external queue if not.

In the basis machine, since the specific SCXML model and transitions are not present, the flags and guards evaluation is missing. The basis provides a starting point so that these engine events can be extended with the specific model information described above.

## Future Triggers

The basis also provides a mechanism for introducing new triggers. Since these triggers require changes to the trigger queues, which are present from the abstract basis, they cannot be handled by ‘new’ events. Abstract ‘futureInternalTrigger’ and ‘futureExternalTrigger’ events are provided for them to refine. A set of ‘FutureInternalTrigger’ and ‘FutureExternalTrigger’ are provided as an abstraction of the triggers that may be introduced in the future.

## 

New triggers are introduced by partitioning this set, leaving a residual for further future triggers



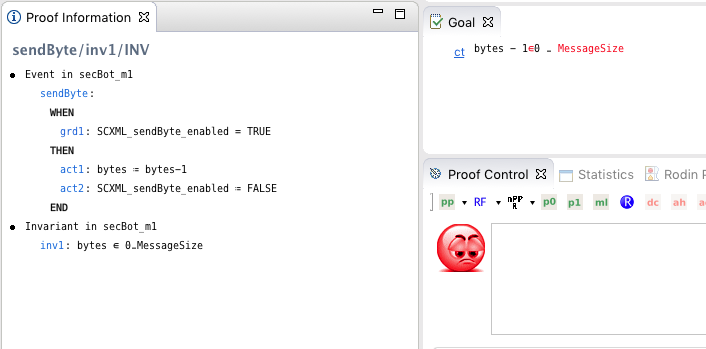
## Refinement of triggers

Note that internal triggers must be introduced as such. They cannot be introduced as external triggers and then later refined as internal ones. This is because the categorisation affects the priority and ordering of their consumption and hence the trace of events which is the definition of refinement. I.e. it is inherently not a refinement to replace an external trigger with an internal trigger. However, an internal trigger can be fired non-deterministically by an un-triggered and unguarded transition. This means that it would be available to fire at any time to enter the event in the queue and later constrained to a specific transition but that the processing of it by the engine would be consistent in future refinements.

## Proof that transitions satisfy invariants

Removing the guards to the SCXML engine means that it is less obvious that transitions satisfy invariants.

For example, the transition sendByte is enabled by the engine when bytes>0. and bytes is not decreased elsewhere. However, the prover cannot initially discharge the PO concerning the range of bytes.



Adding an invariant as follows allows automatic proof.

⚬ inv6: SCXML\_sendByte\_enabled = TRUE ⇒ bytes > 0 not theorem

If another transition decremented bytes, it would not satisfy this invariant.

# Answers to Questions

* *Highest Level*
  + *At this level of abstraction, spi\_done looks like an external event. It won’t be; it comes from elsewhere in the ASIC. However, leaving the transition unguarded makes it look like it should exit the state as soon as it enters it, which is also quite false. What is the appropriate way to represent this?*

In Event-B it is best to leave it unguarded since it is up to you how you interpret the event and when it is likely to occur. I.e. in this case you can interpret the transition as happening sometime in the future as a response to spi\_done. However, the SCXML semantics defines an engine that drives the transition, forcing its execution when its guard is true and removing some of the non-determinism. It cannot be an external event since removing an event from the queue later would break the refinement. (It might be possible to refine the event queues with new ones but the execution traces would also change). In fact it is best to model it as an internal event right from the start and add an always enabled transition to raise spi\_bot non-deterministically. However, I am not sure how best to do the transition in SCXML

* + *Similarly, how can we indicate that the transition from the Wait 50 ms state to the Go state isn’t dependent on an external event, but nonetheless doesn’t happen right away?*

As above, SCXML isn’t designed for refinement. There is a possible way suggested in the next answer. But for Wait50ms it might be best to model it as an external event representing a hardware interrupt.

* + *Perhaps we leave all the transitions unguarded. Then is there any way at this level of detail to express some of those details to be filled in later? (I.e. you know that it’s going to move on when some event indicates it’s ready, you just haven’t captured that behavior yet)*

You could perhaps have some Boolean data items that are used as guards and set them non-deterministically using some un-guarded transition, t. Later the Boolean would be refined by some other data or internal event and the transition t would be refined by the added detail that sets that data or raises the event.

* *First Refinement*
  + *Adding a parallel state is not a vertical refinement. However, this type of design process, wherein the designer starts with the high level flow and then adds details of the communication protocol later, is quite natural. It would not make sense to represent the SPI subsystem as a substate of any of the states on the left-hand side, because it would then have to be duplicated multiple times – once for each state that sends a SPI message.*

Adding an independent state-machine is a valid refinement. Less clear about a parallel state but I think it is ok because the only way it affects the existing state is to restrict its enabledness.

* + *Similar to last slide, there are events whose source is unclear. In this case, send\_message will be raised by some of the states on the left, and last\_byte\_sent will be something that happens inside the Sending Message state. If we leave both of those events out altogether, that will allow the SPI subsystem to churn out messages at arbitrary times. Is that a necessary evil at this level? How should this statechart be represented?*

This is valid and fairly common in abstract models. One way to make the abstract model behave is to use some more abstract data representation such as Boolean flags.

* *Second Refinement*
  + *In some parts of the state machine, a transition must happen and must happen immediately. For example, when send\_message is raised, the SPI subsystem must start transmitting the message, or else the whole statechart will freeze up. It also is necessary that one of the two parallel state machines be able to stay in a single state indefinitely while the other takes various actions. Are these inconsistent? Do they, together, compromise stuttering-invariance and, in turn, refinement?*

It sounds fine to me. Why would the other state-machine need to change state?

The new state-machine contributes new behaviour that expands stuttering in the abstract level. As long as it converges it can stutter as much as it likes.

* + *Is there a scoping problem because send\_message is generated at a different level of refinement than it is responded to?*

Yes, there is. You cannot generate an event without responding to it and then add the response later. (In terms of my Event-B representation, it would mean modifying and abstract variable in a new transition, which is not allowed). You either need to leave out the raising of the send\_message event until later or introduce some abstract transition to respond to it without adding details until later.

* + *There is an intuitive notion that the message is composed of some integer number of bytes, and each byte should be sent sequentially until the last one. The way it is notated right now though is in terms of an event called last\_byte\_sent, which doesn’t indicate that. If we leave off the events altogether, the looping arrow around Send Byte becomes unnecessary, and it looks like it’s only sending one byte. Or an arbitrary number of bytes. How to notate this?*

Not sure I understand the model here. Where are the events ‘last\_byte\_sent’ and ‘!last\_byte\_sent’ raised? Are events an appropriate way to model this? I assumed some local data and un-triggered guarded events here.. but I may have misunderstood the SCXML transition firing.

* *Because of stuttering, the counter isn’t obligated to count. That makes it pretty useless as a delay element. That’s ok for refinement (after all, the thing will eventually be hardware clocked), but it might be a stumbling point for a designer trying to understand it*

Not sure I understand. Maybe we have different ideas of stuttering. How would you guard the transition to Go if you don’t have the count? Anyway, if it is hardware clocked it is probably better to model it as an external trigger event from the start (that’s what I did before I saw refinement 2).