Responses to Reviewers' Comments

for paper titled
Formal verification and validation of run-to-completion style state-charts using Event-B
by
K. Morris, C. Snook, T.S.Hoang, G. Hulette, R. Armstrong, and M. Butler

Thanks We would like to thank the anonymous reviewers for their constructive comments and providing us with the chance to improve our paper. Below we summarise our major changes and address the problems and questions raised by the referees.

Reviewer #1:

```
Presentation
This paper presents an embedding of statecharts in Event-B. As such, it can
be considered as a shallow embedding of statecharts in Event-B. A strong
point of the paper is to adress through refinements the derivation of a
concrete application. The starting point being the basic semantics of the
execution model of statecharts and the last refinement being the considered
application at a given level of detail. Moreover, the paper goes beyond the
usual safety properties usually addressed by such approaches : liveness
properties are here considered.
From my point of view, the presented work is valuable. Actually, it
can be considered as emerging from the synthesis of three conference papers
[12,13,14].
```

Response: ...

" ... "

Reviewer #1:

```
Discussion
  I would appreciate if the authors could elaborate their work along the
  following points:
  - Semantics. Statecharts have a long history. By now, they can be
  considered as belonging to the family of synchronous languages. It
  would be interesting if the authors could give some comments on the
  choice of statecharts and especially on the relevance of the considered
  semantics of run-to-completion. Otherwise stated could the authors
  highlight the benefits of such a choice in general and of stachecharts
  especially.
```

Response: ...

" ... "

Reviewer #1:

- Proof of temporal properties. Different temporal properties are considered. Since the proof of such properties are outside (currently) the Event-B method they have considered other tools and methods.
It would have been interesting to outline the frontier. As a matter of fact, it is not clear for me if the Event-B properties can be tackled in temporal logic, e.g., how sequences are embedded? Could you be precise, comment your embedding?

Response: ...

“ ... ”

Reviewer #1:

- Proof of fairness properties. In order to deal with fairness properties you advocate a strong fairness assumption. From my point a view, this is a strong operating assumption. May be you could comment on that?
Last, but may be I am wrong, I have the intuition that weak fairness for the events handling dequeuing external triggers would be enough?
Please could you comment?

Response: ...

“ ... ”

Reviewer #1:

• p.2 The three rules are not at the same level. The first ones are expressed explicitely in terms of Event-B refinement features, while the third one addresses statecharts.

Response: ...

“ ... ”

Reviewer #1:

• p. 10 typo? listing 3 l. 10 \emptyset

Response: ...

“ ... ”

Reviewer #1:

• p.13 Could you illustrate the sentence all possible combinations of each set of transitions that can fire together are calculated and corresponding events are generated, at appropriate refinement levels.

Response: ...

“ ... ”

Reviewer #1:

- p.15 Fig. 5 is too small. One cannot read its text.

Response: ...

“ ... ”

Reviewer #1:

- p.18 It would have been interesting to state the discussion of the first paragraph of section 7: Verification of Safety Properties within the context of the proof obligation generator you have at hand.

Response: ...

“ ... ”

Reviewer #1:

- p.19 Could you precise your notion of run.

Response: ...

“ ... ”

Reviewer #1:

- p. 20 typo. We are now present

Response: ...

“ ... ”

Reviewer #1:

- p. 21 Could you give a formal definition or at least a reference of your strong fairness.

Response: ...

“ ... ”

Reviewer #1:

- p.22 Could you comment on your definition of anticipated events. Why the set of convergent events is necessary to recall just before?

Response: ...

“ ... ”

Reviewer #1:

- p.22 Proof of Convergence an Anticipation I wonder if this paragraph should not be before because you use such arguments before just after stating Theorem 2.

Response: ...

“ ... ”

Reviewer #1:

- `p.23 typo. it will be dequeued.`

Response: ...

“ ... ”

Reviewer #1:

- `p. 23 could you explain the square bracket notation, e.g. [externalTrigger.t]`

Response: ...

“ ... ”

Reviewer #1:

- `typo. they do no hold a priori.`

Response: ...

“ ... ”

Reviewer #1:

- `typo. relying on lexicographic order . . .`

Response: ...

“ ... ”

Reviewer #1:

- `The paragraph Proof of Convergence and Anticipation needs to be written again. There are many typos: this event removes, discards, decreases, accroding, . . .`
`Moreover the sentence`
`The external events are anticipated accroding to the above variants trivially since they only modify the external queue eQ. Note that we do not attempt to prove the convergence of any future events here. Instead, we assume that these future events will be prove to be convergence later. seems to me problematic. In your definition of anticipated you did not say that these events should be proven convergent later?`

Response: ...

“ ... ”

Reviewer #1:

• p.25 could you state explicitly your strong fairness property and the interplay with the temporal properties you are concerned with.

Response: ...

“ ... ”

Reviewer #1:

• p.25 A reference to the seminal Unless of Unity could be in order.

Response:

Karla: →**Son** Please change in the manuscript

“ ... ”

Reviewer #1:

• p. 26 (Theorem 5) I think that the indexes in eQ should be first stated as legal in both quantifications.

Response:

Karla: →**Son** Please change in the manuscript

“ ... ”

Reviewer #1:

• p. 27 All the temporal proofs have been done in an adhoc way without any tool support. It would be interesting to have a feedback about this? To be provocative, if you are interested in temporal proofs why did you choose this tool? Have you considered TLA which does support temporal proofs (as well as refinements in a certain way)?

Response:

Karla: →**Son** Add some comments of the complexity of the models and and translating them to TLA

Karla: →**Son** Add to manuscript in the related work section TLA

“ ... ”

Reviewer #1:

• It would be interesting to analyze if the proofs are specific to the example or to the underlying semantics?
PS Could you put another zip version on the repository: I have had some strange problems (missing characters) with some machine files? For such files, I was not able to play again the proofs.

Response:

Karla: →**Son** Rephrace in page 23 second bullet point the fact that the variant is model specific. Add a couple of sentences on the semantic nature of the other variants

" ... "

Reviewer #2:

```
The paper introduces a technique for the refinement of 'run to completion'
statechart modelling notation (using SCXML language) while preserving safety
properties. The statechart specification is translated to event-B formalism,
allowing for formal verification using a theorem prover. The proposed approach
is demonstrated using a statechart specification of a drone.

Positive points:
+ Interesting topic
+ Technique well motivated
+ The paper is well written and easy to read.

Negative points:
- One single case study is not enough to validate the proposed approach. The
statechart specification of the drone is rather small. More elaborated models
are required to validate the proposed approach.
```

Response:

Karla: Add references to previous case studies. Make a case that the case studies have grown in complexity and the thje drone in particular makes use of all the features for model construction and refinement. SecBot and Turnstile

" ... "

Reviewer #2:

```
General comments:
  - The three refinement rules listed in the introduction have not been
  described explicitly in the rest of the paper. Please describe them (using
  minimal examples) in section 3.
```

Response:

Karla: Add section 3.2 for refinement rules

" ... "

Reviewer #2:

```
  - In the introduction, the paragraph before last "Page 3: lines 7 to 17" that
  compares the proposed approach to the work presented in [4] may be pushed to
  Section 3 or 4 since such comparison is meaningless before presenting the
  details of the approach and the example.
```

Response: ...

" ... "

Reviewer #2:

- The paper lacks a related work section. Please add one.

Response: A related work section has been added to the manuscript. Please see section

“ ... ”

Reviewer #2:

Minor points:

- After an introductory word or phrase, use a comma (this is a recurrent in the paper). For example, e.g. --> e.g., i.e. --> i.e., "To verify liveness we outline" --> "To verify liveness, we outline", etc.

Response: ...

“ ... ”

Reviewer #2:

- Abstract: "We introduce" --> "In this paper, we introduce".

Response: ...

“ ... ”

Reviewer #2:

- Add "Even-B" to the list of keywords.

Response: ...

“ ... ”

Reviewer #2:

- Page 2: line 5: "Particularly attractive is providing" --> "Particularly attractive in providing"

Response: ...

“ ... ”

Reviewer #2:

- Page 2: line 10: "safety preservation" --> "safety properties preservation"

Response: ...

“ ... ”

Reviewer #2:

- Page 2: line 20: "Preservation of safety" --> "Preservation of safety properties"

Response: ...

“ ... ”

Reviewer #2:

- Page 2: line 45: "in the sense of [9]" --> "in the sense adopted by Lamport [9]"

Response: ...

“ ... ”