TODO - Address comment in DETECT version

DONE - Address comment in DETECT version

LEAVE – Reviewer talking rubbish

LEAVE – Not enough space - Address comment in Journal version

LEAVE – Typesetters will fix

----------------------- REVIEW 1 ---------------------

SUBMISSION: 4

TITLE: Formal verification of run-to-completion style statecharts using Event-B

AUTHORS: Karla Morris, Colin Snook, Thai Son Hoang, Geoffrey C. Hulette, Rob Armstrong and Michael Butler

----------- Overall evaluation -----------

SCORE: 2 (accept)

----- TEXT:

Summary:

The paper introduces a technique for the refinement of `run to completion' statechart modelling notation (using SCXML language) while preserving critical properties, e.g., safety. 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:

- The statechart specification of the drone is rather small. More elaborated models are required to validate the proposed approach.

General comments:

- The three refinement rules listed in the introduction and have not been described explicitly in the rest of the paper. It will be good to state which rule is applied for which refinement in Sections 4.

- In the introduction, the paragraph before last (AlthoughΓÇª.Safety critical systems) that compares the proposed approach to the work presented in [4] may be pushed further in the paper since such comparison is meaningless before presenting the details of the approach and the example.

Typos:

- Introduction: ΓÇÿthis can done byΓÇÖ -> ΓÇÿthis can be done byΓÇÖ

----------------------- REVIEW 2 ---------------------

SUBMISSION: 4

TITLE: Formal verification of run-to-completion style statecharts using Event-B

AUTHORS: Karla Morris, Colin Snook, Thai Son Hoang, Geoffrey C. Hulette, Rob Armstrong and Michael Butler

----------- Overall evaluation -----------

SCORE: 2 (accept)

----- TEXT:

The authors introduce a new notion of refinement into a ΓÇ£run to completionΓÇ¥ state chart-modelling notation, and leverage Event-B's tool support for theorem proving.

They achieved a deep literature analysis to examine the current state-of-the-art of formal refinement and rigorous verification methods in state-chart notations with ΓÇÿrun to competition semanticsΓÇÖ. The literature is comprehensive, rigorous and recent.

The authors show a state-chart representation of how the basis enforces the run to completion semantics on the model transitions. The abstract representation of run to completion basis is clear and refined. However, the authors did not specify why choosing SCML among other modelling languages following `run to completion' semantics.

The State-chart of the drone application is clear and allows to efficiently proving properties of the model in a strategic fashion. It has shown how the refinement of reactive State charts could be translated to Event-B for verification.

-No comparison to other refinement approaches was provided in this paper.

- The word “futureUntriggeredTransitionSet” is in the margins of the page (page 5, to be corrected).

----------------------- REVIEW 3 ---------------------

SUBMISSION: 4

TITLE: Formal verification of run-to-completion style statecharts using Event-B

AUTHORS: Karla Morris, Colin Snook, Thai Son Hoang, Geoffrey C. Hulette, Rob Armstrong and Michael Butler

----------- Overall evaluation -----------

SCORE: 2 (accept)

----- TEXT:

The idea of using Event-B as a semantic back end for a language is

interesting. The adhoc approach followed by the authors seems to show

that the result is manageable and an end user can interact through the

obtained translation and the use of temporal logic for assessing

temporal properties : safety and liveness ones.

Although the SCXML translation is well explained, one would like to

see a formal semantics and the proof that the intended deterministic

propertis are actually esablished by the proposed restrictions.

As said in the introduction, Statecharts is popular with engineers and

variants appear in tools like Matlab Simulink/Stateflow or provided by

Ansys. So one would like to see a comparison between the development

proposed by such tools and a development based on Event-B. A feedback

by some end users would be welcome.

It would have been more interesting to provide the pdf files of the

contexts, the machines and a snapshot of the discharged proofs than

the bare project files.

typo: The SCXML translation tool will then automatically STRENGTHEN

----------------------- REVIEW 4 ---------------------

SUBMISSION: 4

TITLE: Formal verification of run-to-completion style statecharts using Event-B

AUTHORS: Karla Morris, Colin Snook, Thai Son Hoang, Geoffrey C. Hulette, Rob Armstrong and Michael Butler

----------- Overall evaluation -----------

SCORE: 2 (accept)

----- TEXT:

The paper presents a tool for translating SCXML state-chart models into Event-B, via UML-B, to permit automatic verification

of safety properties.

The run to completion semantics and the specific type of refinement being supported are well described.

Overall, the technical aspects are clear. However, some aspects could be better described:

==

2.1 SCXML - " An external trigger may only be consumed when the internal trigger queue has been emptied."

Does this mean that handling internal triggers can introduce lovelock into the system, starving the external triggers from being handled?

3 Run To Completion - "For simplicity, since we do not rely on the exact order of trigger consumption, we use sets to abstractly represent the trigger queues. In Section 7 we will discuss the limitations of this abstraction and the ways in which they can be overcome."

I found it strange that this problem was not addressed until the end of the paper. If the abstraction is limited then why not

fix the abstraction.

- " It may seem that finalisation could cause an unmanageable explosion of guards. However, in practice, the number

of transitions that can fire in parallel is limited (especially for triggered transitions)."

This requires more justification, as it is not clear what is meant by "in practice" .. is it in the case studies that they have

validated the approach on?

4 Description of the Sample Application -

"As part of this design stage we introduce a requirement to constrain drone operation to a battery charge of at least 20% capacity. "

This additional requirement appears to be a simple strengthening of a guard and so is clearly a type of refinement.

However, what if new requirements are not of this nature?

5 SCXML Translation to Event-B

It is nice to have an automated tool chain; but this also introduces maintenance issues for the software development process.

If changes need to be made to requirements or design then which of the 3 models do you work with?

This is a common issue in MDD.

6 Verification of Safety Properties

"To ensure that this reaction is not bypassed by the non-determinism that we incorporated to allow for future refinement, we flag it as finalised at refinement level 2. Finalisation means that we cannot strengthen its guards in future refinements as is normally permitted, since its reaction is needed to ensure the invariant is preserved."

I can see that this works in theory, but does it not introduce unnecessary constraints to the development process.

7 Verification of Control Responses

"an assumption of strong fairness is added for all other events in the model"

is this a reasonable assumption to make?

"After making these changes the final form of the LTL property, which ProB was able to exhaustively check and confirm was as follows:

G([ExternalTriggerEvent decreaseCharge] Γêº {BATTERYOK=TRUE Γêº chargeΓëÑ10 Γêº offΓêê/SCXML dtΓê¬SCXML eq} ΓçÆ F {charge < old(charge)}) ."

But this is not the same as the original requirement -

"G ([ExternalTriggerEvent decreaseCharge] ΓçÆ F {charge < old(charge)}) ."

Does this mean the original requirement was not right? Was it not well specified? This needs further discussion.

==

----------------------- REVIEW 5 ---------------------

SUBMISSION: 4

TITLE: Formal verification of run-to-completion style statecharts using Event-B

AUTHORS: Karla Morris, Colin Snook, Thai Son Hoang, Geoffrey C. Hulette, Rob Armstrong and Michael Butler

----------- Overall evaluation -----------

SCORE: 0 (borderline paper)

----- TEXT:

The authors propose an approach for verifying the ΓÇ£run-to-completion styleΓÇ¥ statecharts using the formal language Event-B.

- The idea of the paper seems interesting.

- The structure of the paper helps the readers to understand the proposed contributions.

- The manuscript is appropriate for the workshop

- The paper does not contain a related work section to compare the proposed contributions with existing works.

- The paper lacks the formal verification of the transformation rules from the State-Chart to Event-B.

- The paper lacks a description of the implementation of the transformation rules. These transformations can be implemented using model-to-model transformation.

- The future work needs to be extended

- The link at the conclusion section is wrong.

- The references need to be accurate and complete