Collins Aerospace

Darren Cofer <darren.cofer@rockwellcollins.com>

[External] ERTS 2020 notification for paper 76

3 messages

ERTS2020 <erts2020@easychair.org> Mon, Sep 16, 2019 at 10:03 AM
To: Darren Cofer <darren.cofer@collins.com>

Dear Darren Cofer,

On behalf of the ERTS 2020 Programme Committee, we are delighted to inform you that your submission:

76 : Safety Annex for the Architecture Analysis and Design Language

has been accepted for publication as regular paper and presentation at the conference provided your final full paper addresses the reviewers and program committee's comments.

We remind you that this acceptance is still conditional. All accepted papers must follow a “shepherding” process. This means that:
- A PC member has been designated to help "shepherd" your paper through this process. We will send you the name and contact details of your assigned shepherd.
- A complete version of the paper should be submitted by Oct 15th to the shepherd. If this delay is not respected, the paper will be rejected.
- The final version of your paper may be rejected by the shepherd if not complying with expectations

Please read carefully the reviews and the shepherding process instructions below.

Shepherding process instructions :
1) In the next days : Your shepherd will contact you in order to provide you with the synthesis of potential improvements to your paper. Feel free to contact your shepherd directly if you do not receive this feedback.
2) October 15th: provide the final version of your paper to your shepherd, taking in account the reviews below and the improvement suggestions
3) Until November 10th: exchange with your shepherd to finalise your paper
4) Before November 10th: upload your paper into the easychair system
5) November 10th: The shepherd informs the program chairs about final acceptance.

The reviews and comments are attached below.

If you have any question, please feel free to get in touch with us.

Best Regards,
On behalf of the ERTS-2020 Programme Committee,
Jean Arlat and ERTS 2020 scientific programme coordination team

SUBMISSION: 76
TITLE: Safety Annex for the Architecture Analysis and Design Language

---------- REVIEW 1 ----------
SUBMISSION: 76
TITLE: Safety Annex for the Architecture Analysis and Design Language
AUTHORS: Danielle Stewart, Jing Liu, Darren Cofer, Mats Heimdahl, Michael Whalen and Michael Peterson

---------- Overall evaluation ----------
SCORE: 2 (accept)
---------- Relevance to ERTS ----------
SCORE: 4 (excellent)
---------- Originality/Novelty ----------
SCORE: 4 (excellent)
---------- Positioning wrt the state of the art ----------
SCORE: 4 (good)

---------- Quality of the presentation ----------
SCORE: 4 (good)
---------- Technical soudness ----------
SCORE: 4 (good)
---------- Candidate for paper award ----------
SCORE: 0 (none)
---------- Applicative domain ----------
Aerospace
---------- Type ----------
SCORE: 3 (Tools / Technology provider)
---------- Review ----------
The paper is very well written and presents an interesting, alternative approach for safety analysis based on the compositional verification method introduced in previous work. However, even though some AADL examples are presented a presentation of the core concepts available in the AADL safety analysis annex would be helpful. In particular, to compare the concepts with concepts which are already available in AADL, for example, to carry out FTA etc.
---------- Ways of improvement for the shepherding process ----------
See above.

---------- REVIEW 2 ----------
SUBMISSION: 76
TITLE: Safety Annex for the Architecture Analysis and Design Language
AUTHORS: Danielle Stewart, Jing Liu, Darren Cofer, Mats Heimdahl, Michael Whalen and Michael Peterson

---------- Overall evaluation ----------
SCORE: 2 (accept)
---------- Relevance to ERTS ----------
SCORE: 4 (excellent)
---------- Originality/Novelty ----------
SCORE: 3 (good)
---------- Positioning wrt the state of the art ----------
SCORE: 4 (good)
---------- Quality of the presentation ----------
SCORE: 5 (excellent)
---------- Technical soudness ----------
SCORE: 4 (good)
---------- Candidate for paper award ----------
SCORE: 0 (none)
---------- Applicative domain ----------
Application domain :
- aviation systems but can be extended to any critical systems
- safety analysis for any critical systems
MBSE
---------- Type ----------
SCORE: 3 (Tools / Technology provider)
---------- Review ----------
This paper présents a study to improve safety analysis of critical systems.

It is based on model-based system engineering : the principles is to extend the use of AADL (modeling of system behaviour to the modeling of component failures.

Among the different methodologies that are Under studies or developement, this paper promote a very efficient methodology thta allow very quick iterations (a few minutes) betwwen systems and the designers.
---------- Ways of improvement for the shepherding process ----------
The paper is very clear.
Thank you very much to present a simple example.

We would like to understand how the fault model is described. Which kind of fault can be put into the model, simple or complex fault behaviour ?

The paper can also define the limitations of the methodology : type of fault, can human behaviour be introduced in the model ...?

---------- REVIEW 3 ----------
SUBMISSION: 76
TITLE: Safety Annex for the Architecture Analysis and Design Language
AUTHORS: Danielle Stewart, Jing Liu, Darren Cofer, Mats Heimdahl, Michael Whalen and Michael Peterson

---------- Overall evaluation ----------
SCORE: 2 (accept)
---------- Relevance to ERTS ----------
SCORE: 4 (excellent)
---------- Originality/Novelty ----------
SCORE: 3 (good)
---------- Positioning wrt the state of the art ----------
SCORE: 4 (good)
---------- Quality of the presentation ----------
SCORE: 4 (good)
---------- Technical soudness ----------
SCORE: 4 (good)
---------- Candidate for paper award ----------
SCORE: 2 (Processes, methods and tools)
---------- Applicative domain ----------
Critical Systems Design (Avionics, but also possibly others like automotive)
---------- Type ----------
SCORE: 1 (Academics)
---------- Review ----------
The paper preents a new extension of the AADL language for Safety annotations.
The annex is a new extension diffrenet for the well known Error annex. It is designed to support safety analyses and is supported by devoted tools to support requiremenst imposed by ARP4754A and ARP4761.

Th idea is to help better integration of safety concerns in the early design stages.

The idea is not really new there has been a lot of work in MBSE-MBSA connections already (Hip-Hops, COMPASS, SOPHIA),....
ModelBased safety analysis is also currently practiced using Cecilia Occas and Altarica frameworks.

In the automotive domains similar approaches have been considered in the context of the EAST-ADL language (ATTEST, 1 and 2, MAENAD, SAFE European projects).

The choice here is to integrate safety annotations within the design model itself whereas in other approaches, such annotations are applied to the design model but not mixed within the model itself.

This provides advantages but also drwbacks mainly for ureuse and/or evaluation of differet possibles alternative solutions.

The paper presents the approach in a clear manner though a summary of the concepts present in the annex would be appreciated.
A discussion on the benefits of the approach regarding concurrent solutions could improve the paper (notably regarding Compass environment).
It could also include a part regarding usability of this approach from the point of vuiew of engineers and how they handle these new features in conjunction with the already existing error annex.
How do you think it will impact process/engineering organization?

The paper should be accepted
---------- Ways of improvement for the shepherding process ----------
The paper presents the approach in a clear manner though a summary of the concepts present in the annex would be appreciated.
A discussion on the benefits of the approach regarding concurrent solutions could improve the paper (notably regarding Compass environment).

It would be interesting to get a feedback from the point of view of engineers (designesr and safety specialists) on possible evolutions in their organizations and processes.

Darren Cofer <darren.cofer@collins.com> Mon, Sep 16, 2019 at 10:17 AM

Reply-To: darren.cofer@collins.com
To: Janet Liu <Jing.Liu@rockwellcollins.com>, Mats Heimdahl <heimdahl@umn.edu>, Danielle Stewart <dkstewar@umn.edu>

Darren Cofer
Collins Aerospace
319-263-2571
darren.cofer@collins.com
[Quoted text hidden]

Mats Heimdahl <heimdahl@umn.edu> Mon, Sep 16, 2019 at 10:18 AM
Reply-To: heimdahl@umn.edu
To: Darren Cofer <darren.cofer@collins.com>
Cc: Janet Liu <Jing.Liu@rockwellcollins.com>, Danielle Stewart <dkstewar@umn.edu>

Saw it. Thank you Darren.

Mats
[Quoted text hidden]
--
Mats Heimdahl, Professor and Department Head
Department of Computer Sci. and Eng. Phone: (612)-625-2068
College of Science and Engineering Dept.: (612)-625-4002
University of Minnesota, Twin Cities Fax : (612)-625-0572
4-192 Keller Hall. 200 Union Street S.E. Minneapolis, MN 55455