Translation validation for a Lustre compiler

Keywords: translation validation, code generation, Lustre

1 Team and advisors

The project will take place at ISAE-SUPAERO in Toulouse, France, in the Department of Complex Systems Engineering (DISC), more precisely in the Design and Analysis of Critical Systems team (CASC). The advisors will be Prof. Xavier Thirioux and Dr. Christophe Garion.

2 Context

CoCoSim is a NASA Ames, ISAE-SUPAERO and ENAC joint effort to develop a platform for Simulink/Stateflow code generation and validation. CoCoSim generates Lustre code form Simulink/Stateflow models and we are developing Lustrec, an academic compiler from Lustre with several backends, e.g. to low level languages such as C or SPARK or Horn clauses for formal verification. The overall objective of CoCoSim is to formally prove properties such as contracts or invariants on models or code artifacts. In order to do that, the first step is of course to ensure the correctness of the generated code.

This postdoctorate position is part of the CLEDESCHAMPS project funded by french Ministry of Defense. The aim of this project is to develop efficient compilation and validation tools for software embedded on UAV. CLEDESCHAMPS is also part of a joint effort including similar projects from École Polytechnique, ENSTA Paris and ENSTA Bretagne.

3 Objectives

The LustreC compiler has a C backend and we have currently added an ACSL generation plugin to instrument the generated code. This ACSL specification mainly states the correctness of the generated C code, both with respect to Lustre semantics and also with respect to high level functional contracts expressed on Lustre code.

The objectives of the current postdoctorate position are the following:

1. extend the current ACSL generation scheme to Lustre constructions such as arrays
2. extend the current ACSL generation scheme to handle more aggressive optimizations
3. allow the verification of functional properties expressed as Lustre contracts *à la* Kind2

4 Expected skills

The applicant should have a PhD in Computer Science on one or more of the following domains: compilation, formal verification, formal proof. Experience in OCaml programming will be appreciated.

5 Practical details

The position is open for 18 months starting from september 2022. The corresponding salary is about 2100 per month tax deducted. Applicants must be EU nationals.

6 Contacts

- Christophe Garion, ISAE-SUPAERO/DISC
- Xavier Thirioux, ISAE-SUPAERO/DISC

References

[1] Hamza Bourbouh et al. "From Lustre To Simulink". In: *ACM Transactions on Cyber-Physical Systems* 5.3 (2021), pp. 1–20. DOI: 10.1145/3461668. URL: https://doi.org/10.1145/3461668.

[2] Guillaume Davy et al. "Preserving Functional Correctness of Cyber-Physical System Controllers: From Model to Code". In: *2018 Forum on Specification & Design Languages, FDL 2018*. Ed. by Hiren Patel, Tom J. Kazmierski, and Sebastian Steinhorst. IEEE, 2018, pp. 5–16. ISBN: 978-1-5386-6418-6. DOI: 10.1109/FDL.2018.8524044.

[3] Pierre-Loïc Garoche, Temesghen Kahsai, and Xavier Thirioux. "Hierarchical State Machines as Modular Horn Clauses". In: *Proceedings 3rd Workshop on Horn Clauses for Verification and Synthesis*. Ed. by John P. Gallagher and Philipp Rümmer. Vol. 219. EPTCS. 2016, pp. 15–28. DOI: 10.4204/EPTCS.219.2.